

Rec'd PCT/PTO 19 OCT 2004

10/511751

日 本 国 特 許 庁
JAPAN PATENT OFFICE

PCT/JP03/04808

16.04.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年 4月23日

出 願 番 号
Application Number:

特願2002-120430

[ST.10/C]:

[JP2002-120430]

出 願 人
Applicant(s):

松下電器産業株式会社

REC'D 13 JUN 2003

WIPO

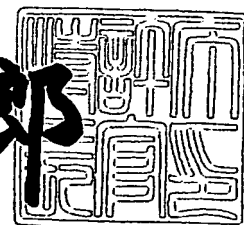
PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 5月27日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



BEST AVAILABLE COPY

出証番号 出証特2003-3038956

【書類名】 特許願
 【整理番号】 2032740027
 【提出日】 平成14年 4月23日
 【あて先】 特許庁長官殿
 【国際特許分類】 G06F 9/06
 G06F 15/16
 G06F 12/14

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 前田 卓治

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 三浦 康史

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 徳田 克己

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 井上 信治

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 プログラム更新及び管理方法

【特許請求の範囲】

【請求項 1】 情報処理端末を一意に識別する端末 ID を外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、前記情報処理端末で動作するプログラム、前記プログラムに関する情報を格納したプログラムヘッダ、前記プログラムが使用する固有の情報であるプログラム固有情報、前記プログラム固有情報に関する情報を格納した固有情報ヘッダを保持するサーバ装置との間で行われるプログラム更新及び管理方法であって、

前記情報処理端末は、前記サーバ装置に対して前記端末 ID を含んだプログラム配布要求を行い、

前記サーバ装置は、前記プログラム配布要求に対して前記プログラム、前記プログラムヘッダ、前記プログラム固有情報、前記固有情報ヘッダを配布することを特徴とするプログラム更新及び管理方法。

【請求項 2】 前記情報処理端末はさらに、

前記情報処理端末内の外部から書き換えが行えない不揮発性メモリに前記情報処理端末毎に異なる固有鍵を格納し、

前記サーバ装置から取得した前記プログラムを、前記固有鍵を用いて暗号化して前記情報処理端末内に格納することを特徴とする請求項 1 記載のプログラム更新及び管理方法。

【請求項 3】 前記プログラムヘッダは前記プログラムを一意に特定することが可能な認証子を含み、前記固有鍵で暗号化され前記情報処理端末内に格納されているプログラムを前記固有鍵で復号し、前記認証子を用いて固有鍵での暗号化が正しく行われたことを確認することを特徴とする請求項 2 記載のプログラム更新及び管理方法。

【請求項 4】 前記プログラム、前記プログラムヘッダ、前記プログラム固有情報、前記固有情報ヘッダは電子的な署名が付加されていることを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載のプログラム更新及び管理方法。

【請求項 5】 前記プログラムヘッダは前記プログラムを一意に特定することが

可能な認証子を含み、前記固有情報ヘッダは前記プログラム固有情報を一意に特定することが可能な認証子を含み、前記プログラムヘッダ、前記固有情報ヘッダは電子的な署名が付加されていることを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載のプログラム更新及び管理方法。

【請求項 6】 情報処理端末を一意に識別する端末 ID を外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、前記プログラム固有情報を配布した情報処理端末を一意に識別する端末 ID と前記情報処理端末に配布した前記プログラム固有情報を一意に識別するプログラム固有情報 ID の対応を示す固有情報配布履歴を保持するサーバ装置との間で行われるプログラム更新及び管理方法であって、

前記情報処理端末からの端末 ID を指定したプログラム配布要求に対し、前記固有情報配布履歴に記載されている情報処理端末からの要求であれば前記プログラムのみを配布し、

前記固有情報配布履歴に記載されていない情報処理端末からの要求であれば前記プログラムと共に新規に前記プログラム固有情報を割り当てて配布し、

前記固有情報配布履歴に前記端末 ID、前記プログラム固有情報 ID の対応関係を追加することを特徴とするプログラム更新及び管理方法。

【請求項 7】 前記プログラム固有情報は特定のプログラムに関連付けられた情報であり、前記プログラム固有情報 ID と前記プログラムを一意に識別するプログラム ID の対応を示すプログラム／固有情報対応表と、前記固有情報配布履歴を保持するサーバ装置において、前記情報処理端末からの端末 ID とプログラム ID を指定したプログラム配布要求に対し、前記プログラム／固有情報対応表と前記固有情報配布履歴を参照し、指定された前記プログラム ID に対応する前記プログラム固有情報を前記情報処理端末に配布済みであれば前記プログラムのみを配布し、配布していなければプログラムと共に新規に前記プログラム固有情報を割り当てて配布し、前記固有情報配布履歴に前記端末 ID、前記プログラム固有情報 ID の対応関係を追加することを特徴とする請求項 6 記載のプログラム更新及び管理方法。

【請求項 8】 情報処理端末を一意に識別する端末 ID を外部から書き換えが行

えない不揮発性メモリに格納する情報処理端末と、前記プログラム固有情報を配布した情報処理端末を一意に識別する端末IDと、前記端末IDを持つ情報処理端末に対してプログラム固有情報を配布した回数の対応を示す配布回数情報を保持するサーバ装置との間で行われるプログラム更新及び管理方法であって、

前記情報処理端末からの端末IDを指定したプログラム配布要求に対し、前記配布回数情報に記載されている配布回数が規定値以上であれば前記プログラムのみを配布し、規定値未満であれば前記プログラムと共に新規に前記プログラム固有情報を割り当てて配布し、前記配布回数情報に記載されている配布回数を更新することを特徴とするプログラム更新及び管理方法。

【請求項9】前記プログラム固有情報は特定のプログラムに関連付けられた情報であり、前記プログラム固有情報IDと前記プログラムを一意に識別するプログラムIDの対応を示すプログラム／固有情報対応表と、前記配布回数情報を保持するサーバ装置において、前記情報処理端末からの端末IDとプログラムIDを指定したプログラム配布要求に対し、前記プログラム／固有情報対応表と前記配布回数情報を参照し、指定された前記プログラムIDに対応する前記プログラム固有情報を前記情報処理端末に配布した回数が規定値以上であれば前記プログラムのみを配布し、規定値未満であればプログラムと共に新規に前記プログラム固有情報を割り当てて配布し、前記配布回数情報に記載されている配布回数を更新することを特徴とする請求項8記載のプログラム更新及び管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理端末で動作するプログラムの更新方法に関し、プログラムの配布方法、ならびに配布したプログラムの管理方法に関する。

【0002】

【従来の技術】

近年、携帯電話からのインターネット接続や、デジタルTVの放送開始など、ネットワークサービスに対応した組込み機器が登場し、注目を浴びている。ネットワーク技術の発展によりネットワークのブロードバンド化が進む中、ネットワ

ークサービスに対応した組込み機器は今後さらに登場するものと考えられる。

【0003】

組込み機器のネットワーク化に伴い機器が急速に高機能化されるにつれ、各機器に搭載されるソフトウェアの規模は飛躍的に増大している。ソフトウェアの大規模化は、開発人員の増加、開発工数の長期化などの諸問題を引き起こす。また、ネットワークサービス提供者間の競争により新規サービスが次々と登場する中、端末メーカーも新規サービスに対応した新機種を短期間で開発することが求められており、機器の開発サイクルは短くなってきている。

【0004】

このような背景により、端末メーカーは大規模なソフトウェアを短期間に開発、テストし、商品を出荷する必要がある。結果として機器に対する十分なテストが行えないまま市場に出荷され、後日ソフトウェアの不具合が発覚し、商品回収を行うというケースも増加している。

【0005】

従来、組込み機器におけるプログラムの不具合修正方法としては、商品を回収してプログラムを入れ替える方法が存在する。商品を回収してプログラムを入れ替える方法では、回収した商品に対しプログラムを格納しているROMを張り替えたり、プログラムを格納しているFlashメモリのプログラムを新しいプログラムに書き換えたりすることで、プログラムの不具合修正を行う。この方法では、ユーザが店頭に商品を持参する、商品をメーカーに送付するなどの必要がありユーザにかかる負担は大きい。また、回収コストも膨大になるため、ユーザ、メーカーの両者にとって商品を回収せずに修正する方法が望ましい。

【0006】

一方、組込み機器がネットワークに接続されることにより、ネットワークから様々なデータを取得し、ネットワークを用いたサービスを利用することが可能になる。例えばホームページの閲覧や、電子メールの送受信、音楽・画像などのコンテンツ配信サービスなど、従来PCで実現されていたネットワークサービスが組込み機器で実現できるほか、組込み機器の機能と組み合わせた新規サービスの実現も可能となる。また、ネットワークから取得する情報はデータだけではなく

、プログラムを取得することも可能である。そのため、従来機器の回収という形で行ってきたプログラムの不具合修正を、ネットワーク経由のプログラム配信により実現することが可能になる。また、従来PCで行われてきた、ネットワーク経由のプログラム追加による機能追加を組み込み機器で実現することも可能になる。

【0007】

【発明が解決しようとする課題】

電子ショッピングやコンテンツ配信サービスなど、課金を伴う商用システムを実現する場合、悪意のあるユーザが不正にプログラムを書き換えることが可能であれば、課金情報の操作により無料で商品やコンテンツを購入するなどの不正行為が行われる可能性がある。そのため、ネットワーク経由のプログラム更新による不具合修正、追加を行う場合、悪意のあるユーザが不正に改ざんしたプログラムを機器に取り込まないように、プログラムの正当性を検証する必要がある。

【0008】

従来プログラムの正当性を検証する方法として、特開2000-339153号公報に示されるような電子的な署名を用いる方法が存在する。この方法では、公開鍵暗号方式と呼ばれる2つの対となる鍵の組を用いた暗号化データ交換方式を利用する。署名を用いたプログラムの正当性検証方法に関して、図1を用いて説明する。同図において、100はプログラムを開発し配布するプログラム発行者、110はプログラム発行元の身元を確認し保証する第三者認証機関であるCA (Certification Authority)、120はプログラムを取得するユーザを示す。プログラム発行者100は、公開鍵101、秘密鍵102と呼ばれる2つの鍵を保有する。秘密鍵102はプログラム発行者100のみが知り得る鍵であり、プログラム発行者100が秘匿情報として管理する。公開鍵101は他者に公開するための鍵であり、公開しても秘密鍵102の内容は予測できない仕組みとなっている。CA 110はプログラム発行者100と同じく、CA公開鍵111、CA秘密鍵112の2つの鍵を保有する。

【0009】

プログラム正当性検証の手順は次の通り。

【0010】

(1) プログラム発行者100はCA110に公開鍵101を送付する。

【0011】

(2) CA110は、プログラム発行者100の身元を確認、審査する。

【0012】

(3) CA110がプログラム発行者100を信頼できると判断した場合、プログラム発行者100の公開鍵101に対しCA秘密鍵112で電子的な署名を行った証明書を発行する。証明書は公開鍵保有者の身元を識別する情報を含み、第三者認証機関であるCA110が公開鍵保有者の身元を保証するものである。

【0013】

(4) CA110は、プログラム発行者100にプログラム発行者の公開鍵証明書103を送付する。

【0014】

(5) プログラム発行者100は配布するプログラムに対し、自己の秘密鍵101で電子的な署名を行う。

【0015】

(6) プログラム発行者100はユーザ120に対し、公開鍵証明書103、署名付きプログラム104を配布する。

【0016】

(7) ユーザ120はCA110からCA公開鍵111を取得する。

【0017】

(8) ユーザ120は、CA公開鍵111を用いてプログラム発行者の公開鍵証明書103の署名を検証する。

【0018】

(9) 署名の検証が正しく行われた場合、公開鍵証明書103に含まれる公開鍵101を用いて署名付きプログラム104の署名を検証する。

【0019】

(10) 署名の検証が正しく行われた場合、配布されたプログラムがプログラム発行者100から配布されたプログラムであり、改ざんされていないことを検

証できる。上記の公開鍵暗号方式及び証明書、署名、認証の仕組みに関しては、「Applied Cryptography」Bruce Schneier, John Wiley & Sons, Inc (1996) が詳しい。

【0020】

ここで説明した方法では、文書に手書きの署名を付加し、正当性を保証すると同様に、プログラムに電子的な署名を付加することによりプログラムの正当性を保証している。これにより、ユーザ120はプログラムが配布元から発行された正当なものであることを検証できる。

【0021】

しかしながら、図1に示した例では配布時におけるプログラムの正当性検証は行えるが、配布後のプログラムに関して正当性を保証することはできない。この問題点を解決する方法として、特開平7-295800号公報が存在する。特開平7-295800号公報に示された方法は、プログラム配布先のユーザ識別子を用いてプログラム配布元でプログラムを暗号化して配布し、ユーザは使用時にユーザ識別子を用いてプログラムを復号化して実行する方法である。この方法では、万が一プログラムが不正にコピーされたとしても、ユーザ識別子が一致しなければプログラムを復号し実行することができないため、不正コピー、不正改ざんを防止することが可能となる。しかしながら、プログラム配布元で各ユーザ識別子に応じた暗号処理を行う必要があり、プログラム配布元にかかる負担は大きい。

【0022】

一方、ネットワークを用いた電子ショッピングや、コンテンツ配信サービスなど、課金を伴う商用システムを実現する場合、ユーザを特定する方法が必要となる。そのため、プログラムあるいはプログラムと共に配布する情報の中に、ユーザ毎に割り当てるIDや鍵などの固有情報を含ませる場合がある。この場合、ユーザに固有情報を割り当て、管理することで、ユーザが不正行為を行った際に固有情報を元にユーザを特定することが可能となる。不正ユーザを特定すれば、不正ユーザが使用する固有情報を無効にすることで、不正行為を防止することが可能となる。

【 0 0 2 3 】

この固有情報を用いた不正行為を防止する方法では、1 ユーザが複数の固有情報を取得することが可能であれば、不正ユーザとして排除されたユーザが再度別の固有情報を取得することで、新たなユーザとして識別され、更に不正行為を繰り返すことが可能となるため。そのため、不正ユーザが複数の固有情報を取得できないようにする仕組みが必要となる。

【 0 0 2 4 】

本発明では上記問題点に鑑み、プログラム配布元の負担が少ないプログラムの不正コピーや不正改ざんを防ぐ方法を提供すると共に、固有情報のユーザへの配布回数を制限することで不正行為を防止することが可能なプログラム更新及び管理方法を提供することを目的とする。

【 0 0 2 5 】

【課題を解決するための手段】

前記課題を解決するために第1の発明は、情報処理端末を一意に識別する端末IDと、情報処理端末毎に異なる固有鍵を外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、情報処理端末で動作するプログラム、プログラムに関する情報を格納したプログラムヘッダ、プログラムが使用する固有の情報であるプログラム固有情報、プログラム固有情報に関する情報を格納した固有情報ヘッダを保持するサーバ装置において、情報処理端末の端末IDを含んだプログラム配布要求に対し、それぞれ電子的な署名が付加されたプログラム、プログラムヘッダ、プログラム固有情報、固有情報ヘッダを配布し、情報処理端末内でプログラムを固有鍵で暗号化し格納することを特徴とする。

【 0 0 2 6 】

前記課題を解決するために第2の発明は、プログラムヘッダにプログラムを一意に特定することが可能な認証子を含み、固有情報ヘッダにプログラム固有情報を一意に特定することが可能な認証子を含み、プログラムヘッダと固有情報ヘッダに電子的な署名を付加することを特徴とする。

【 0 0 2 7 】

前記課題を解決するために第3の発明は、プログラム固有情報を配布した情報

処理端末を一意に識別する端末IDと、情報処理端末に配布したプログラム固有情報を一意に識別するプログラム固有情報IDの対応を管理する固有情報配布履歴を保持するサーバ装置において、情報処理端末からの端末IDを指定したプログラム配布要求に対し、固有情報配布履歴に記載されている情報処理端末からの要求であればプログラムのみを配布し、固有情報配布履歴に記載されていない情報処理端末からの要求であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、固有情報配布履歴に端末ID、プログラム固有情報IDの対応関係を追加することを特徴とする。

【0028】

前記課題を解決するために第4の発明は、プログラム固有情報を一意に識別するプログラム固有情報IDと、プログラムを一意に識別するプログラムIDの対応を示すプログラム／固有情報対応表と、固有情報配布履歴を保持するサーバ装置において、情報処理端末からの端末IDとプログラムIDを指定したプログラム配布要求に対し、プログラム／固有情報対応表と固有情報配布履歴を参照し、指定されたプログラムIDに対応するプログラム固有情報を配布済みの情報処理端末からの要求であればプログラムのみを配布し、配布していない情報処理端末からの要求であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、固有情報配布履歴に端末ID、プログラム固有情報IDの対応関係を追加することを特徴とする。

【0029】

前記課題を解決するために第5の発明は、プログラムが使用するプログラム固有情報を配布した情報処理端末を一意に識別する端末IDと、プログラム固有情報を配布した回数を示す配布回数情報を保持するサーバ装置において、情報処理端末からの端末IDを指定したプログラム配布要求に対し、配布回数情報に記載されている配布回数が規定値以上であればプログラムのみを配布し、規定値未満であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、配布回数情報に記載されている配布回数を更新することを特徴とする。

【0030】

前記課題を解決するために第6の発明は、プログラム固有情報を一意に識別す

るプログラム固有情報IDと、プログラムを一意に識別するプログラムIDの対応を示すプログラム／固有情報対応表と、配布回数情報を保持するサーバ装置において、情報処理端末からの端末IDとプログラムIDを指定したプログラム配布要求に対し、プログラム／固有情報対応表と配布回数情報を参照し、指定されたプログラムIDに対応するプログラム固有情報を情報処理端末に配布した回数が規定値以上であればプログラムのみを配布し、規定値未満であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、配布回数情報に記載されている配布回数を更新することを特徴とする。

【0031】

【発明の実施の形態】

以下、本発明のプログラム更新及び管理方法について、図を用いて説明する。

【0032】

(実施の形態1)

図2は本発明の実施の形態1における情報処理端末とサーバ装置の構成図であり、同図において、200は情報処理端末、220はサーバ装置を示している。情報処理端末200は、CPU201、RAM202、プログラムやデータなどの暗号化及び復号化処理を行う暗号処理部203、サーバ装置220との通信を行う通信処理部204、プログラムを格納するプログラム格納部205、CA公開鍵など特に秘匿する必要がない情報を格納するデータ格納部206、秘密鍵など秘匿する必要がある情報を格納する秘匿情報格納部207から構成されている。プログラム格納部205には、CPU201で動作するプログラム216が格納されている。データ格納部206は、情報処理端末200で使用されるデータのうち特に秘匿する必要がないものが格納されており、情報処理端末200に格納されているプログラムのIDやバージョン番号など格納プログラムの管理情報であるプログラム管理情報208、CA公開鍵209が格納されている。また、秘匿情報格納部207は、情報処理端末200内で秘匿する必要がある情報が格納されており、情報処理端末毎に異なる鍵である端末固有鍵210、情報処理端末毎に異なる公開鍵ペアの1つである端末秘密鍵211、プログラムが使用する固有鍵などのプログラム固有情報212、情報処理端末毎に異なる公開鍵ペアの

他方である端末公開鍵証明書 213 が格納されている。端末公開鍵証明書 213 は情報処理端末を一意に識別する ID である端末 ID 214、端末公開鍵証明書に対し CA が付加した CA 署名 215 を含んでいる。

【0033】

一方サーバ装置 220 は、CPU 221、RAM 222、プログラムやデータなどの暗号化及び復号化処理を行う暗号処理部 223、情報処理端末 200 との通信を行う通信処理部 224、CA 公開鍵など特に秘匿する必要がない情報を格納するデータ格納部 225、情報処理端末 200 に配布するプログラムなどの情報を格納する配布情報格納部 226 から構成されている。さらにデータ格納部 225 はサーバ装置 220 が使用する情報を格納する領域であり、公開鍵ペアの 1 つであるサーバ秘密鍵 227、公開鍵ペアの他方であるサーバ公開鍵証明書 228、CA 公開鍵 229 が格納されている。サーバ公開鍵証明書 228 はサーバを一意に識別する ID であるサーバ ID 230、サーバ公開鍵証明書に対し CA が付加した CA 署名 231 を含んでいる。配布情報格納部 226 は、サーバ装置 220 が情報処理端末 200 に対して配布する情報を格納する領域であり、プログラムヘッダ 232、プログラム 233、固有情報ヘッダ 234、プログラム固有情報 235 が格納されている。

【0034】

配布情報格納部 226 に格納されているプログラムヘッダ 232、プログラム 233、固有情報ヘッダ 234、プログラム固有情報 235 には第三者認証機関である CA の署名が付加されており、配布情報が正当な配布元から配布されるものであることを保証している。

【0035】

次に図 3 を用いて、プログラムヘッダとプログラムの関係を説明する。

【0036】

プログラムヘッダ 300 は、プログラム 310 に関する情報を格納するものである。プログラムヘッダ 300 は、次の情報を含む。

【0037】

(1) プログラムヘッダ 300 が格納する情報がどのプログラム 310 に対応

した情報かを示すプログラムID (301)。

【0038】

(2) 対応するプログラム310のバージョン番号 (302)。

【0039】

(3) 対応するプログラム310のプログラムサイズ (303)。

【0040】

(4) 対応するプログラム310のハッシュ値 (304)。

【0041】

(5) 上記(1)から(4)までの情報を含むプログラムヘッダ300全体に対するCAの署名 (305)。

【0042】

また、プログラム310は、プログラム310に対するCAの署名 (311) が付加されている。

【0043】

このようにプログラムヘッダ300、プログラム310は共にCAの署名を含むため、情報処理端末200においてプログラムヘッダ、プログラムが正当な配布元から配布されたものであることを検証することが可能である。

【0044】

同様に図4を用いて、固有情報ヘッダとプログラム固有情報の関係を説明する。

【0045】

固有情報ヘッダ400は、プログラム固有情報420に関する情報を格納するものである。固有情報ヘッダ400は、次の情報を含む。

【0046】

(1) 固有情報ヘッダ400が格納する情報がどのプログラム固有情報420に対応した情報かを示すプログラム固有情報ID (401)。

【0047】

(2) 対応するプログラム固有情報420を使用するプログラムのプログラムID (402)。

【0048】

(3) 対応するプログラム固有情報420が格納する固有情報の数(403)

【0049】

(4) 対応するプログラム固有情報420全体のサイズ(404)。

【0050】

(5) 対応するプログラム固有情報420に含まれる個々の固有情報に関する情報を示す固有情報サブヘッダ(405)。固有情報サブヘッダ405はプログラム固有情報420に含まれる個々の固有情報の数だけ存在する。

【0051】

(6) 上記(1)から(5)までの情報を含む固有情報ヘッダ400全体に対するCAの署名(406)。

【0052】

固有情報サブヘッダ405はさらに個々の固有情報を識別するためのIDであるプログラム固有情報サブID411、個々の固有情報のサイズ412から構成される。

【0053】

また、プログラム固有情報420は、複数のプログラム固有情報(421)と、プログラム固有情報全体に対するCAの署名(422)を含む。

【0054】

このように固有情報ヘッダ400、プログラム固有情報420は共にCAの署名を含むため、情報処理端末200において固有情報ヘッダ、プログラム固有情報が正当な配布元から配布されたものであることを検証することが可能である。

【0055】

次に情報処理端末200、サーバ装置220間で行われるプログラム更新手順の例を、図5を用いて説明する。

【0056】

第1にS501において、情報処理端末200とサーバ装置220はSSL(Secure Socket Layer)による接続を行う。SSLは、2点

間でデータを安全に送受信するために、公開鍵暗号方式と秘密鍵暗号方式を併用して、データを暗号化して送受信する仕組みである。SSLの詳細はNetscape社から技術文書として公開されている。SSLではセッション鍵と呼ばれる鍵を共有するため、S502以降の情報処理端末200とサーバ装置220間のデータ送受信は、すべてセッション鍵を用いた暗号化データにより行われる。

【0057】

次にS502において、情報処理端末200はサーバ装置220に対し、取得したいプログラム233のプログラムIDを指定してヘッダの取得を要求する。

【0058】

S503において、ヘッダ取得要求を受信したサーバ装置220は、配布情報格納部226に格納したプログラムヘッダ232を情報処理端末200に送信する。

【0059】

S504において、サーバ装置220からプログラムヘッダ232を受信した情報処理端末200は、データ格納部206に格納しているCAの公開鍵209を用いて、プログラムヘッダ232に含まれているCAの署名を検証する。これにより、情報処理端末200はプログラムヘッダ232が改ざんされていない、正当な配布元から配布された情報であることを検証する。プログラムヘッダ232には、プログラムのプログラムID、バージョン番号、サイズ、プログラムのハッシュ値などプログラムに関する情報が格納されている。この情報と、データ格納部206に格納されているプログラム管理情報208内に記載されているプログラムID、バージョン情報、空き容量情報を比較し、更新対象のプログラムが正しくサーバ装置220から配布されたか、プログラムを格納する空き容量が存在するか確認する。

【0060】

次にS505において、サーバ装置220は配布情報格納部226に格納した固有情報ヘッダ234を情報処理端末200に送信する。

【0061】

S506において、サーバ装置220から固有情報ヘッダ234を受信した情

報処理端末 2 0 0 は、データ格納部 2 0 6 に格納している C A の公開鍵 2 0 9 を用いて、固有情報ヘッダ 2 3 4 に含まれている C A の署名を検証する。これにより、情報処理端末 2 0 0 は固有情報ヘッダ 2 3 4 が改ざんされていない、正当な配布元から配布された情報であることを検証する。固有情報ヘッダ 2 3 4 には、プログラム固有情報を一意に識別するプログラム固有情報 I D、プログラム固有情報に関連するプログラムのプログラム I D、プログラム固有情報で配布される情報に含まれる固有情報の数、サイズなどプログラム固有情報に関する情報が格納されている。この情報と、データ格納部 2 0 6 に格納されているプログラム管理情報 2 0 8 内に記載されているプログラム I D、空き容量情報を比較し、更新対象のプログラムに関するプログラム固有情報が正しくサーバ装置 2 2 0 から配布されたか、プログラム固有情報を格納する空き容量が存在するか確認する。

【 0 0 6 2 】

S 5 0 4、S 5 0 6 で情報処理端末 2 0 0 が空き容量の確認を行い、プログラム、プログラム固有情報の取得が行えると判断した場合、S 5 0 7 において情報処理端末 2 0 0 はサーバ装置 2 2 0 に対しプログラム I D を指定してプログラム取得を要求する。

【 0 0 6 3 】

S 5 0 8 において、プログラム取得要求を受信したサーバ装置 2 2 0 は、配布情報格納部 2 2 6 に格納したプログラム 2 3 3 を情報処理端末 2 0 0 に送信する。

【 0 0 6 4 】

次に S 5 0 9 において、サーバ装置 2 2 0 からプログラム 2 3 3 を受信した情報処理端末 2 0 0 は、データ格納部 2 0 6 に格納している C A の公開鍵 2 0 9 を用いて、プログラム 2 3 3 に含まれている C A の署名を検証する。これにより、情報処理端末 2 0 0 はプログラム 2 3 3 が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム 2 3 3 を秘匿情報格納部 2 0 7 に格納している端末固有鍵 2 1 0 で暗号化し、プログラム格納部 2 0 5 に格納する。その際、プログラム格納位置やプログラム I D、バージョン番号などをプログラム管理情報 2 0 8 に格

納し、プログラムの管理を行う。

【0065】

S510において、プログラムの格納が完了した後、プログラム格納部205に格納したプログラム216を、端末固有鍵210を用いて復号し、ハッシュ値を算出する。算出した値とプログラムヘッダ232に格納されているハッシュ値の比較を行い、プログラムが正しく格納されていることを確認する。

【0066】

次にS511において情報処理端末200はサーバ装置220に対しプログラムIDを指定してプログラム固有情報取得を要求する。

【0067】

S512において、サーバ装置220は配布情報格納部226に格納したプログラム固有情報235を情報処理端末200に送信する。

【0068】

次にS513において、サーバ装置220からプログラム固有情報235を受信した情報処理端末200は、データ格納部206に格納しているCAの公開鍵209を用いて、プログラム固有情報235に含まれているCAの署名を検証する。これにより、情報処理端末200はプログラム固有情報が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム固有情報を秘匿情報格納部207に格納する。

【0069】

プログラム、プログラム固有情報の格納が完了した後、通信を切断する（S514）。

【0070】

図5で示した本発明のプログラム更新手順について、本発明の主眼となる点について説明する。

【0071】

第1に情報処理端末200においてプログラムを暗号化している点である。従来の方法ではサーバ装置220においてプログラムを情報処理端末200固有の

鍵で暗号化していたため、サーバ装置 2 2 0 においてプログラムを暗号化する処理が必要であった。これに対し本発明では情報処理端末 2 0 0 においてプログラムを暗号化しているため、サーバ装置 2 2 0 におけるプログラム暗号化処理の負担を軽減することが可能となる。

【 0 0 7 2 】

また、情報処理端末 2 0 0 において情報処理端末 2 0 0 固有の鍵である端末固有鍵 2 1 0 で暗号化した場合、正しく端末固有鍵 2 1 0 で暗号化が行えたことを確認する必要がある。この点に関し本発明では、プログラム格納後に端末固有鍵 2 1 0 で復号し、平文プログラムのハッシュ値による検証を行う。復号後のプログラムに対するハッシュ値を検証することで、情報処理端末 2 0 0 毎に異なる端末固有鍵暗号化を意識することなく、プログラム格納の成否を判定することが可能となる。

【 0 0 7 3 】

第 2 にプログラムとプログラム固有情報を個別に作成している点である。端末毎に異なる情報であるプログラム固有情報は、複数端末に配布するため複数の情報を管理する必要があるが、プログラムを利用する全端末で共通な情報となるプログラムは 1 式のみ管理することになる。これにより、サーバ装置 2 2 0 で管理する配布情報の大きさを低減することが可能となり、サーバ装置 2 2 0 における情報管理の負担を軽減することが可能となる。

【 0 0 7 4 】

なお、本実施の形態では情報処理端末 2 0 0 とサーバ装置 2 2 0 間で SSL を用いた暗号化データの送受信を行っているが、2 点間で安全にデータの送受信が行える方法であれば、SSL に限らず他のプロトコルを用いてもよい。また、本実施の形態ではデータ格納部 2 0 6 とプログラム格納部 2 0 5 を別に行っているが、同一の格納部としてもよい。また、本実施の形態では秘匿情報格納部 2 0 7 に端末公開鍵証明書 2 1 3 を格納しているが、データ格納部 2 0 6 に格納してもよい。また、本実施の形態ではプログラムヘッダ、固有情報ヘッダをプログラム、プログラム固有情報とは別に作成しているが、プログラムとプログラムヘッダ、プログラム固有情報と固有情報ヘッダをそれぞれ一体の情報とし、サーバ装置 2

20からの配布に先立ちヘッダ部分のみ切り出して情報処理端末200に送信してもよい。また、本実施の形態ではプログラム、プログラム固有情報に対し配布時にセッション鍵による暗号化を行う例を示したが、セッション鍵とは異なる鍵でさらに暗号化し、その鍵をプログラムヘッダ、固有情報ヘッダに含めて配布する構成としてもよい。また、本実施の形態でハッシュ値と記載している点は、ハッシュアルゴリズムとしてSHA-1、MD5などの既存のハッシュアルゴリズムを使用してもよいし、独自のアルゴリズムを用いてもよい。また、ハッシュアルゴリズムのかわりにチェックサムなどの方法を用いて改ざんの検出を行ってもよい。また、情報処理端末200毎に異なる情報を必要としないプログラムを配布する場合は、プログラム固有情報の配布を行う必要はない。

【0075】

(実施の形態2)

図6、図7は本発明の実施の形態2におけるサーバ装置220内の配布情報格納部226に格納されるデータを示す。情報処理端末200とサーバ装置220の構成は、本発明の実施の形態1と同様、図2に示すものとする。

【0076】

図6を用いて、プログラムヘッダとプログラムの関係を説明する。

【0077】

プログラムヘッダ600は、プログラム610に関する情報を格納するものである。プログラムヘッダ600は、次の情報を含む。

【0078】

(1) プログラムヘッダが格納する情報がどのプログラムに対応した情報かを示すプログラムID(601)。

【0079】

(2) 対応するプログラムのバージョン番号(602)。

【0080】

(3) 対応するプログラムのプログラムサイズ(603)。

【0081】

(4) 対応するプログラムのハッシュ値(604)。

【0082】

(5) 上記(1)から(4)までの情報を含むプログラムヘッダ全体に対するCAの署名(605)。

【0083】

本発明の実施の形態1と異なる点は、プログラム610にCAの署名を付加しない点である。

【0084】

プログラムヘッダ600、プログラム610の正当性検証を情報処理端末200において行う場合、次の手順で行う。

【0085】

第1にプログラムヘッダ600をサーバ装置220から取得し、プログラムヘッダ600に付加されたCAの署名605を検証する。これにより、情報処理端末200はプログラムヘッダ600が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【0086】

次にプログラム610のハッシュ値を算出する。算出したハッシュ値と、プログラムヘッダ600に格納されているプログラムのハッシュ値604を比較し、一致することを確認する。これにより、情報処理端末200はプログラム610が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【0087】

このように、プログラム610の正当性検証にプログラムヘッダ600に格納されたプログラムのハッシュ値604を使用し、プログラムヘッダ600にのみCA署名605を付加することで、CAの署名を必要とする情報を低減しながら、プログラムヘッダ600、プログラム610に署名を付加する場合と同様の効果を得ることが可能となる。

【0088】

また、プログラムヘッダ600とプログラム610の組み合わせが不正に変更された場合、情報処理端末200において、プログラムのハッシュ値を算出する

ことにより組み合わせの異常を検出することが可能となる。

【0089】

次に図7を用いて、固有情報ヘッダとプログラム固有情報の関係を説明する。

【0090】

固有情報ヘッダ700は、プログラム固有情報720に関する情報を格納するものである。固有情報ヘッダ700は、次の情報を含む。

【0091】

(1) 固有情報ヘッダが格納する情報がどのプログラム固有情報に対応した情報かを示すプログラム固有情報ID(701)。

【0092】

(2) 対応するプログラム固有情報を使用するプログラムのプログラムID(702)。

【0093】

(3) 対応するプログラム固有情報が格納する固有情報の数(703)。

【0094】

(4) 対応するプログラム固有情報全体のサイズ(704)。

【0095】

(5) 対応するプログラム固有情報全体のハッシュ値(705)。

【0096】

(6) 対応するプログラム固有情報に含まれる個々の固有情報に関する情報を示す固有情報サブヘッダ(706)。固有情報サブヘッダ706はプログラム固有情報に含まれる個々の固有情報の数だけ存在する。

【0097】

(7) 上記(1)から(6)までの情報を含む固有情報ヘッダ全体に対するCAの署名(707)。

【0098】

固有情報サブヘッダ706はさらに個々の固有情報を識別するためのIDであるプログラム固有情報サブID711、個々の固有情報のサイズ712から構成される。

【 0 0 9 9 】

本発明の実施の形態 1 と異なる点は、固有情報ヘッダ 7 0 0 にプログラム固有情報 7 2 0 のハッシュ値を格納し、プログラム固有情報 7 2 0 に C A の署名を付加しない点である。

【 0 1 0 0 】

固有情報ヘッダ 7 0 0、プログラム固有情報 7 2 0 の正当性検証を情報処理端末 2 0 0 において行う場合、次の手順で行う。

【 0 1 0 1 】

第 1 に固有情報ヘッダ 7 0 0 をサーバ装置 2 2 0 から取得し、固有情報ヘッダ 7 0 0 に付加された C A の署名 7 0 7 を検証する。これにより、情報処理端末 2 0 0 は固有情報ヘッダ 7 0 0 が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【 0 1 0 2 】

次にプログラム固有情報 7 2 0 のハッシュ値を算出する。算出したハッシュ値と、固有情報ヘッダ 7 0 0 に格納されているプログラム固有情報のハッシュ値 7 0 5 を比較し、一致することを確認する。これにより、情報処理端末 2 0 0 はプログラム固有情報 7 2 0 が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【 0 1 0 3 】

このように、固有情報ヘッダ 7 0 0 にプログラム固有情報のハッシュ値 7 0 5 を格納し、固有情報ヘッダ 7 0 0 にのみ C A 署名 7 0 7 を付加することで、C A の署名を必要とする情報を低減しながら、固有情報ヘッダ 7 0 0、プログラム固有情報 7 2 0 に署名を付加する場合と同様の効果を得ることが可能となる。

【 0 1 0 4 】

また、固有情報ヘッダ 7 0 0 とプログラム固有情報 7 2 0 の組み合わせが不正に変更された場合、情報処理端末 2 0 0 において、プログラム固有情報のハッシュ値を算出することにより組み合わせの異常を検出することが可能となる。

【 0 1 0 5 】

なお、本実施の形態でハッシュ値と記載している点は、ハッシュアルゴリズム

としてSHA-1、MD5などの既存のハッシュアルゴリズムを使用してもよいし、独自のアルゴリズムを用いてもよい。また、ハッシュアルゴリズムのかわりにチェックサムなどの方法を用いて改ざんの検出を行ってもよい。

【0106】

(実施の形態3)

図8に本発明の実施の形態3における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態1と異なる点は、サーバ装置820がプログラム固有情報835を情報処理端末800に配布した履歴を管理するための固有情報配布履歴840を保持する点である。

【0107】

固有情報配布履歴840の情報格納例を図9に示す。

【0108】

固有情報配布履歴900は、プログラム固有情報835を配布した情報処理端末800を識別するIDである端末ID901、配布したプログラム固有情報835を識別するIDであるプログラム固有情報ID902を格納する。また、必要に応じてプログラム固有情報835を最後に配布した日時を示す最終配布日付903を格納する。

【0109】

同図の例では、サーバ装置820は情報処理端末800に5つのプログラム固有情報835を配布済みであり、それぞれの端末ID901、プログラム固有情報ID902の組は、(端末ID、プログラム固有情報ID) = (0001、0001)、(0002、0002)、(0010、0003)、(0015、0004)、(0020、0005)となる。

【0110】

サーバ装置820における固有情報配布履歴840を用いたプログラム配布手順について図10を用いて説明する。

【0111】

第1にS1001において、サーバ装置820は情報処理端末800からプログラム配布要求を受信する。

【0112】

次にS1002において、S1001で受信したプログラム配布要求に含まれる情報処理端末800の端末IDを取得する。

【0113】

S1003において、固有情報配布履歴840に対してS1002で取得した端末IDを検索する。

【0114】

S1004において、固有情報配布履歴840に同じ端末IDが格納されているか否か判定する。

【0115】

固有情報配布履歴840に同じ端末IDが格納されていた場合（S1004でY）、情報処理端末800へは既にプログラム固有情報835を配布済みであるため、S1008においてプログラム833のみを送信し処理を終了する。

【0116】

固有情報配布履歴840に同じ端末IDが格納されていない場合（S1004でN）、S1005において情報処理端末800へは新たにプログラム固有情報835を割り当てる。

【0117】

次にS1006において、S1005で新たに割り当てたプログラム固有情報835に関し、端末IDとプログラム固有情報IDの対応を固有情報配布履歴840に追加する。

【0118】

S1007において、プログラム固有情報835を情報処理端末800に送信し、S1008においてプログラム833を送信し処理を終了する。

【0119】

このようにサーバ装置820において固有情報配布履歴840を用いて配布管理することにより、1つの情報処理端末800へ複数のプログラム固有情報835を配布することを防ぐ。これにより、プログラム固有情報835が含む情報を用いて不正端末と認識され、排除されている情報処理端末800に対し、新たに

プログラム固有情報 8 3 5 を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

【 0 1 2 0 】

なお、本実施の形態ではデータ格納部 8 0 6 とプログラム格納部 8 0 5 を別に行っているが、同一の格納部としてもよい。また、本実施の形態で示した固有情報配布履歴 8 4 0 の形式は一例であり、最終配布日付情報を削除してもよいし、他の情報を付加してもよい。また、本実施の形態では固有情報配布履歴 8 4 0 に記載されている情報処理端末 8 0 0 に対してプログラム固有情報 8 3 5 の配布を拒否しているが、その情報処理端末 8 0 0 に対して既に配布済みのプログラム固有情報 8 3 5 を再度配布してもよい。また、本実施の形態では情報処理端末 8 0 0 からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【 0 1 2 1 】

（実施の形態 4）

図 1 1 に本発明の実施の形態 4 における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態 3 と異なる点は、サーバ装置 1 1 2 0 がプログラム／固有情報対応表 1 1 5 0 を保持する点である。

【 0 1 2 2 】

プログラム／固有情報対応表 1 1 5 0 は、プログラム固有情報を識別するプログラム固有情報 ID と、プログラム固有情報を使用するプログラムのプログラム ID との対応を示した表である。

【 0 1 2 3 】

本発明の実施の形態 4 における固有情報配布履歴 1 1 4 0 と、プログラム／固有情報対応表 1 1 5 0 の例を図 1 2 に示す。

【 0 1 2 4 】

固有情報配布履歴 1 2 0 0 は、プログラム固有情報 1 1 3 5 を配布した情報処理端末 1 1 0 0 を識別する ID である端末 ID 1 2 0 1、配布したプログラム固有情報 1 1 3 5 が対応するプログラム 1 1 3 3 を識別する ID であるプログラム ID 1 2 0 2、配布したプログラム固有情報 1 1 3 5 を識別する ID であるプロ

グラム固有情報ID1203を格納する。また、必要に応じてプログラム固有情報1135を最後に配布した日時を示す最終配布日付1204を格納する。本発明の実施の形態3における固有情報配布履歴と異なる点は、プログラム固有情報を使用するプログラムを識別するプログラムID1202が付加されている点である。

【0125】

図12の例では、サーバ装置1120は情報処理端末1100に5つのプログラム固有情報1135を配布済みであり、それぞれの端末ID1201、プログラムID1202、プログラム固有情報ID1203の組は、(端末ID、プログラムID、プログラム固有情報ID) = (0001、0001、0001)、(0002、0001、0002)、(0010、0001、0003)、(0015、0001、0004)、(0020、0002、1001)となる。

【0126】

またプログラム／固有情報対応表は、サーバ装置1120が管理しているプログラムのプログラムIDと、各プログラムが使用するプログラム固有情報を識別するプログラム固有情報IDの対応関係を格納する。

【0127】

図12の例では、サーバ装置1120はプログラムIDが0001のプログラムを管理しており、そのプログラムが使用するプログラム固有情報としてプログラム固有情報IDが0001から1000までのプログラム固有情報を管理している。同様にプログラムIDが0002のプログラムと、そのプログラムが使用するプログラム固有情報IDが1001から2000までのプログラム固有情報を管理している。また、プログラム／固有情報対応表は、プログラム固有情報をどこまで情報処理端末1100に配布済みであり、次のプログラム固有情報配布の際に、配布すべきプログラム固有情報を示す配布開始ID1213を格納する。

【0128】

図12の例では、プログラムIDが0001のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置1120は0123のプログラム固

有情報IDを持つプログラム固有情報を割り当てることを示している。同様にプログラムIDが0002のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置1120は1423のプログラム固有情報IDを持つプログラム固有情報を割り当てることを示している。

【0129】

本発明の実施の形態4では、サーバ装置1120は、このプログラム／固有情報対応表を元に、情報処理端末1100からのプログラムIDを指定したプログラム配布要求に対し、そのプログラムIDに対応したプログラム固有情報を配布する。

【0130】

本発明の実施の形態4におけるプログラム配布手順について、図13を用いて説明する。

【0131】

第1にS1301において、サーバ装置1120は情報処理端末1100からプログラム配布要求を受信する。

【0132】

次にS1302において、S1301で受信したプログラム配布要求に含まれる情報処理端末1100の端末ID、プログラムIDを取得する。

【0133】

S1303において、固有情報配布履歴1140に対してS1302で取得した端末ID、プログラムIDを検索する。

【0134】

S1304において、固有情報配布履歴1140に同じ端末IDかつ同じプログラムIDの履歴が格納されているか否か確認する。

【0135】

固有情報配布履歴1140に同じ端末IDかつ同じプログラムIDの履歴が格納されていた場合（S1304でY）、情報処理端末1100へは既に指定プログラムに対するプログラム固有情報1135を配布済みであるため、S1309においてプログラムのみを送信し処理を終了する。

【0136】

固有情報配布履歴1140に同じ端末IDかつ同じプログラムIDの履歴が格納されていない場合（S1304でN）、S1305においてプログラム／固有情報対応表1150に格納されている配布開始IDの情報を元に情報処理端末1100へ新たにプログラム固有情報1135を割り当てる。

【0137】

次にS1306において、S1305で新たに割り当てたプログラム固有情報1135に関し、プログラム／固有情報対応表1150に格納されている配布開始IDの値を更新する。

【0138】

また、S1307において、S1305で新たに割り当てたプログラム固有情報1135に関し、端末IDとプログラム固有情報IDの対応を固有情報配布履歴1140に追加する。

【0139】

S1308において、プログラム固有情報1135を情報処理端末1100に送信し、S1309においてプログラム1133を送信し処理を終了する。

【0140】

このようにサーバ装置1120において固有情報配布履歴1140とプログラム／固有情報対応表1150を用いて配布管理することにより、1つの情報処理端末1100で動作する同一プログラムに対して複数のプログラム固有情報1135を配布することを防ぐ。これにより、本発明の実施の形態3と同様に、プログラム固有情報1135が含む情報を用いて不正端末と認識され、排除されている情報処理端末1100に対し、新たにプログラム固有情報1135を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

【0141】

また、本発明の本実施の形態4では、プログラム固有情報1135の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報1135の配布可否を判定することが可能となる。

【0142】

なお、本実施の形態ではデータ格納部 1 1 0 6 とプログラム格納部 1 1 0 5 を別に分けているが、同一の格納部としてもよい。また、本実施の形態で示した固有情報配布履歴の形式は一例であり、最終配布日付情報を削除してもよいし、他の情報を付加してもよい。同様にプログラム／固有情報対応表の形式も一例であり、配布開始 ID を別の形式で管理してもよい。

【 0 1 4 3 】

例えば、全プログラム固有情報 ID を格納したテーブルを持ち、各プログラム固有情報 ID に対して割り当て済みか否かを識別するフラグを設けることにより、プログラム固有情報 1 1 3 5 の配布状態を管理してもよい。また、本実施の形態では固有情報配布履歴 1 1 4 0 に記載されている情報処理端末 1 1 0 0 に対してプログラム固有情報 1 1 3 5 の配布を拒否しているが、その情報処理端末 1 1 0 0 に対して既に配布済みのプログラム固有情報 1 1 3 5 を再度配布してもよい。また、本実施の形態では情報処理端末 1 1 0 0 からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【 0 1 4 4 】

(実施の形態 5)

図 1 4 に本発明の実施の形態 5 における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態 1 と異なる点は、サーバ装置 1 4 2 0 がプログラム固有情報 1 4 3 5 を情報処理端末 1 4 0 0 に配布した回数を管理するための配布回数情報 1 4 4 0 を保持する点である。

【 0 1 4 5 】

図 1 5 に配布回数情報 1 4 4 0 の情報格納例を示す。

【 0 1 4 6 】

配布回数情報 1 5 0 0 は、プログラム固有情報 1 4 3 5 を配布した情報処理端末 1 4 0 0 を識別する ID である端末 ID 1 5 0 1、配布した回数を示す回数カウンタ 1 5 0 2 を格納する。

【 0 1 4 7 】

同図の例では、端末 ID が 0 0 0 1、0 0 0 2 の情報処理端末 1 4 0 0 に対し

てプログラム固有情報 1 4 3 5 を 1 回配布しており、端末 ID が 0 0 0 3 の情報処理端末 1 4 0 0 に対してプログラム固有情報 1 4 3 5 を配布していない。

【0 1 4 8】

サーバ装置 1 4 2 0 における配布回数情報 1 4 4 0 を用いたプログラム配布手順について図 1 6 を用いて説明する。

【0 1 4 9】

第 1 に S 1 6 0 1 において、サーバ装置 1 4 2 0 は情報処理端末 1 4 0 0 からプログラム配布要求を受信する。

【0 1 5 0】

次に S 1 6 0 2 において、S 1 6 0 1 で受信したプログラム配布要求に含まれる情報処理端末 1 4 0 0 の端末 ID を取得する。

【0 1 5 1】

S 1 6 0 3 において、配布回数情報 1 4 4 0 に対して S 1 6 0 2 で取得した端末 ID を検索し、回数カウンタの値を取得する。

【0 1 5 2】

S 1 6 0 4 において、取得した回数カウンタの値が規定値以上か否かを判定する。

【0 1 5 3】

取得した回数カウンタの値が規定値以上であった場合 (S 1 6 0 4 で Y)、情報処理端末 1 4 0 0 へは既にプログラム固有情報 1 4 3 5 を規定回数以上配布しているため、S 1 6 0 8 においてプログラム 1 4 3 3 のみを送信し処理を終了する。

【0 1 5 4】

取得した回数カウンタの値が規定値未満であった場合 (S 1 6 0 4 で N)、S 1 6 0 5 において情報処理端末 1 4 0 0 へは新たにプログラム固有情報 1 4 3 5 を割り当てる。

【0 1 5 5】

次に S 1 6 0 6 において、配布回数情報 1 4 4 0 内に格納されている回数カウンタの値を加算する。

【0156】

S1607において、プログラム固有情報1435を情報処理端末1400に送信し、S1608においてプログラム1433を送信し処理を終了する。

【0157】

このようにサーバ装置1420において配布回数情報1440を用いて配布管理することにより、1つの情報処理端末1400へ規定数以上のプログラム固有情報1435を配布することを防ぐ。特に規定値を1に設定した場合、本発明の実施の形態3と同様、プログラム固有情報1435が含む情報を用いて不正端末と認識され、排除されている情報処理端末1400に対し、新たにプログラム固有情報1435を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

【0158】

なお、本実施の形態ではデータ格納部1406とプログラム格納部1405を別に分けているが、同一の格納部としてもよい。また、本実施の形態で示した配布回数情報の形式は一例であり、他の情報を付加してもよい。また、本実施の形態では情報処理端末1400からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【0159】

(実施の形態6)

図17に本発明の実施の形態6における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態5と異なる点は、サーバ装置1720がプログラム／固有情報対応表1750を保持する点である。

【0160】

プログラム／固有情報対応表1750は、プログラム固有情報を識別するプログラム固有情報IDと、プログラム固有情報を使用するプログラムのプログラムIDとの対応を示した表である。

【0161】

本発明の実施の形態6における配布回数情報1740と、プログラム／固有情

報対応表 1 7 5 0 の例を図 1 8 に示す。

【 0 1 6 2 】

配布回数情報 1 8 0 0 は、配布したプログラム固有情報 1 7 3 5 が対応するプログラム 1 7 3 3 を識別する ID であるプログラム ID 1 8 0 1、プログラム固有情報 1 7 3 5 を配布した情報処理端末 1 7 0 0 を識別する ID である端末 ID 1 8 0 2、配布した回数を示す回数カウンタ 1 8 0 3 を格納する。本発明の実施の形態 5 における配布回数情報と異なる点は、プログラム固有情報を使用するプログラムを識別するプログラム ID が付加されている点である。

【 0 1 6 3 】

図 1 8 の例では、プログラム ID が 0 0 0 1 のプログラムが使用するプログラム固有情報 1 7 3 5 を、端末 ID が 0 0 0 1、0 0 0 2 の情報処理端末 1 7 0 0 に対して 1 回配布しており、端末 ID が 0 0 0 3 の情報処理端末 1 7 0 0 に対してプログラム固有情報 1 7 3 5 を配布していない。また同様に、プログラム ID が 0 0 0 2 のプログラムが使用するプログラム固有情報 1 7 3 5 を、端末 ID が 0 0 0 1 の情報処理端末 1 7 0 0 に対して 1 回配布しており、端末 ID が 0 0 0 2、0 0 0 3 の情報処理端末 1 7 0 0 に対してプログラム固有情報 1 7 3 5 を配布していない。

【 0 1 6 4 】

またプログラム／固有情報対応表 1 7 5 0 は、サーバ装置 1 7 2 0 が管理しているプログラムのプログラム ID と、各プログラムが使用するプログラム固有情報を識別するプログラム固有情報 ID の対応関係を格納する。図 1 8 の例では、サーバ装置 1 7 2 0 はプログラム ID が 0 0 0 1 のプログラムを管理しており、そのプログラムが使用するプログラム固有情報としてプログラム固有情報 ID が 0 0 0 1 から 1 0 0 0 までのプログラム固有情報を管理している。同様にプログラム ID が 0 0 0 2 のプログラムと、そのプログラムが使用するプログラム固有情報 ID が 1 0 0 1 から 2 0 0 0 までのプログラム固有情報を管理している。

【 0 1 6 5 】

また、プログラム／固有情報対応表 1 7 5 0 は、プログラム固有情報 1 7 3 5 をどこまで情報処理端末 1 7 0 0 に配布済みであり、次回のプログラム固有情報

配布の際に、配布すべきプログラム固有情報 1 7 3 5 を示す配布開始 ID 1 8 1 3 を格納する。図 1 8 の例では、プログラム ID が 0 0 0 1 のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置 1 7 2 0 は 0 1 2 3 のプログラム固有情報 ID を持つプログラム固有情報を割り当てることを示している。同様にプログラム ID が 0 0 0 2 のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置 1 7 2 0 は 1 4 2 3 のプログラム固有情報 ID を持つプログラム固有情報を割り当てることを示している。

【 0 1 6 6 】

本発明の実施の形態 6 では、サーバ装置 1 7 2 0 は、このプログラム／固有情報対応表 1 7 5 0 を元に、情報処理端末 1 7 0 0 からのプログラム ID を指定したプログラム配布要求に対し、そのプログラム ID に対応したプログラム固有情報 1 7 3 5 を配布する。

【 0 1 6 7 】

本発明の実施の形態 6 におけるプログラム配布手順について、図 1 9 を用いて説明する。

【 0 1 6 8 】

第 1 に S 1 9 0 1 において、サーバ装置 1 7 2 0 は情報処理端末 1 7 0 0 からプログラム配布要求を受信する。

【 0 1 6 9 】

次に S 1 9 0 2 において、S 1 9 0 1 で受信したプログラム配布要求に含まれる情報処理端末 1 7 0 0 の端末 ID、プログラム ID を取得する。

【 0 1 7 0 】

S 1 9 0 3 において、配布回数情報 1 7 4 0 に対して S 1 9 0 2 で取得した端末 ID、プログラム ID を検索し、回数カウンタの値を取得する。

【 0 1 7 1 】

S 1 9 0 4 において、取得した回数カウンタの値が規定値以上か否かを判定する。

【 0 1 7 2 】

取得した回数カウンタの値が規定値以上であった場合（S 1 9 0 4 で Y）、情

報処理端末 1 7 0 0 へは既にプログラム固有情報 1 7 3 5 を規定回数以上配布しているため、S 1 9 0 9 においてプログラム 1 7 3 3 のみを送信し処理を終了する。

【 0 1 7 3 】

取得した回数カウンタの値が規定値未満であった場合（S 1 9 0 4 で N）、S 1 9 0 5 においてプログラム／固有情報対応表 1 7 5 0 に格納されている配布開始 ID の情報を元に情報処理端末 1 7 0 0 へ新たにプログラム固有情報 1 7 3 5 を割り当てる。

【 0 1 7 4 】

次に S 1 9 0 6 において、S 1 9 0 5 で新たに割り当てたプログラム固有情報 1 7 3 5 に関し、プログラム／固有情報対応表 1 7 5 0 に格納されている配布開始 ID の値を更新する。

【 0 1 7 5 】

また、S 1 9 0 7 において、配布回数情報 1 7 4 0 内に格納されている回数カウンタの値を加算する。

【 0 1 7 6 】

S 1 9 0 8 において、プログラム固有情報 1 7 3 5 を情報処理端末 1 7 0 0 に送信し、S 1 9 0 9 においてプログラム 1 7 3 3 を送信し処理を終了する。

【 0 1 7 7 】

このようにサーバ装置 1 7 2 0 において配布回数情報 1 7 4 0 とプログラム／固有情報対応表 1 7 5 0 を用いて配布管理することにより、1 つの情報処理端末 1 7 0 0 で動作する同一プログラムに対して規定数以上のプログラム固有情報 1 7 3 5 を配布することを防ぐ。これにより、本発明の実施の形態 5 と同様に、プログラム固有情報 1 7 3 5 の配布回数を制限することが可能となる。

【 0 1 7 8 】

また、本発明の本実施の形態 6 では、プログラム固有情報の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報の配布可否を判定することが可能となる。

【 0 1 7 9 】

なお、本実施の形態ではデータ格納部とプログラム格納部を別にしているが、同一の格納部としてもよい。また、本実施の形態で示した配布回数情報の形式は一例であり、他の情報を付加してもよい。同様にプログラム／固有情報対応表の形式も一例であり、配布開始IDを別の形式で管理してもよい。また、本実施の形態では情報処理端末からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【0180】

【発明の効果】

以上のように、情報処理端末を一意に識別する端末IDと、情報処理端末毎に異なる固有鍵を外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、情報処理端末で動作するプログラム、プログラムに関する情報を格納したプログラムヘッダ、プログラムが使用する固有の情報であるプログラム固有情報、プログラム固有情報に関する情報を格納した固有情報ヘッダを保持するサーバ装置において、情報処理端末の端末IDを含んだプログラム配布要求に対し、それぞれ電子的な署名が付加されたプログラム、プログラムヘッダ、プログラム固有情報、固有情報ヘッダを配布し、情報処理端末内でプログラムを固有鍵で再暗号化し格納することで、配布後のプログラムを不正改ざんから守ることができる。

【0181】

また、プログラムヘッダにプログラムを一意に特定することが可能な認証子を含み、固有情報ヘッダにプログラム固有情報を一意に特定することが可能な認証子を含み、プログラムヘッダと固有情報ヘッダに電子的な署名を付加することで、全ての情報の署名を付加することなく、情報の正当性検証を行うことができる。

【0182】

また、プログラム固有情報を配布した情報処理端末の端末IDと、情報処理端末に配布したプログラム固有情報のプログラム固有情報IDの対応を管理する固有情報配布履歴をサーバ装置に保持し、複数のプログラム固有情報を1つの情報

処理端末に割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【0183】

また、プログラム固有情報のプログラム固有情報IDと、プログラムのプログラムIDの対応を示すプログラム／固有情報対応表と、固有情報配布履歴をサーバ装置に保持し、複数のプログラム固有情報を、情報処理端末で実行される1つのプログラムに割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【0184】

また、プログラム固有情報を配布した情報処理端末の端末IDと、プログラム固有情報を配布した回数を示す配布回数情報をサーバ装置に保持し、規定数以上のプログラム固有情報を1つの情報処理端末に割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【0185】

また、プログラム固有情報のプログラム固有情報IDと、プログラムのプログラムIDの対応を示すプログラム／固有情報対応表と、配布回数情報をサーバ装置に保持し、規定数以上のプログラム固有情報を、情報処理端末で実行される1つのプログラムに割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【図面の簡単な説明】

【図1】

署名を用いたプログラム正当性検証方法の例を示す図

【図2】

本発明の実施の形態1における情報処理端末とサーバ装置の構成を示す図

【図3】

本発明の実施の形態1におけるプログラムヘッダとプログラムの関係を示す図

【図4】

本発明の実施の形態1における固有情報ヘッダとプログラム固有情報の関係を

示す図

【図 5】

プログラム更新手順の例を示す図

【図 6】

本発明の実施の形態 2 におけるプログラムヘッダとプログラムの関係を示す図

【図 7】

本発明の実施の形態 2 における固有情報ヘッダとプログラム固有情報の関係を示す図

【図 8】

本発明の実施の形態 3 における情報処理端末とサーバ装置の構成を示す図

【図 9】

本発明の実施の形態 3 における固有情報配布履歴の構成を示す図

【図 10】

本発明の実施の形態 3 における固有情報配布履歴を用いたプログラム配布手順を示すフローチャート

【図 11】

本発明の実施の形態 4 における情報処理端末とサーバ装置の構成を示す図

【図 12】

本発明の実施の形態 4 における固有情報配布履歴、プログラム／固有情報対応表の構成を示す図

【図 13】

本発明の実施の形態 4 における固有情報配布履歴、プログラム／固有情報対応表を用いたプログラム配布手順を示すフローチャート

【図 14】

本発明の実施の形態 5 における情報処理端末とサーバ装置の構成を示す図

【図 15】

本発明の実施の形態 5 における配布回数情報の構成を示す図

【図 16】

本発明の実施の形態 5 における配布回数情報を用いたプログラム配布手順を示

すフローチャート

【図 17】

本発明の実施の形態 6 における情報処理端末とサーバ装置の構成を示す図

【図 18】

本発明の実施の形態 6 における配布回数情報、プログラム／固有情報対応表の構成を示す図

【図 19】

本発明の実施の形態 6 における配布回数情報、プログラム／固有情報対応表を用いたプログラム配布手順を示すフローチャート

【符号の説明】

100 プログラム発行者
 110 CA
 120 ユーザ
 101, 111 公開鍵
 102, 112 秘密鍵
 103 プログラム発行者公開鍵証明書
 104 署名付きプログラム
 121, 216, 233, 310, 610, 833, 1133, 1433, 1733 プログラム
 200, 800, 1100, 1400, 1700 情報処理端末
 201, 221, 801, 821, 1101, 1121, 1401, 1421, 1701, 1721 CPU
 202, 222, 802, 822, 1102, 1122, 1402, 1422, 1702, 1722 AM
 203, 223, 803, 823, 1103, 1123, 1403, 1423, 1703, 1723 暗号処理部
 204, 224, 804, 824, 1104, 1124, 1404, 1424, 1704, 1724 通信処理部
 205, 805, 1105, 1405, 1705 プログラム格納部

206, 225, 806, 825, 1106, 1125, 1406, 1425
 , 1706, 1725 データ格納部

207, 807, 1107, 1407, 1707 秘匿情報格納部

208 プログラム管理情報

209, 229, 829, 1129, 1429, 1729 CA公開鍵

210 端末固有鍵

211 端末秘密鍵

212 プログラム固有情報

213 端末公開鍵証明書

214, 901, 1201, 1501, 1802 端末ID

215, 231, 305, 311, 406, 422, 605, 707, 831
 , 1131, 1431, 1731 CA署名

220, 820, 1120, 1420, 1720 サーバ装置

226, 826, 1126, 1426, 1726 配布情報格納部

227, 827, 1127, 1427, 1727 サーバ秘密鍵

228, 828, 1128, 1428, 1728 サーバ公開鍵証明書

230, 830, 1130, 1430, 1730 サーバID

232, 300, 600, 832, 1132, 1432, 1732 プログラ
 ムヘッダ

234, 400, 700, 834, 1134, 1434, 1734 固有情報
 ヘッダ

235, 420, 421, 720, 721, 835, 1135, 1435, 1
 735 プログラム固有情報

301, 402, 601, 702, 1202, 1211, 1801, 1811
 プログラムID

302, 602 バージョン番号

303, 603 プログラムサイズ

304, 604 プログラムハッシュ値

401, 701, 902, 1203, 1212, 1812 プログラム固有情

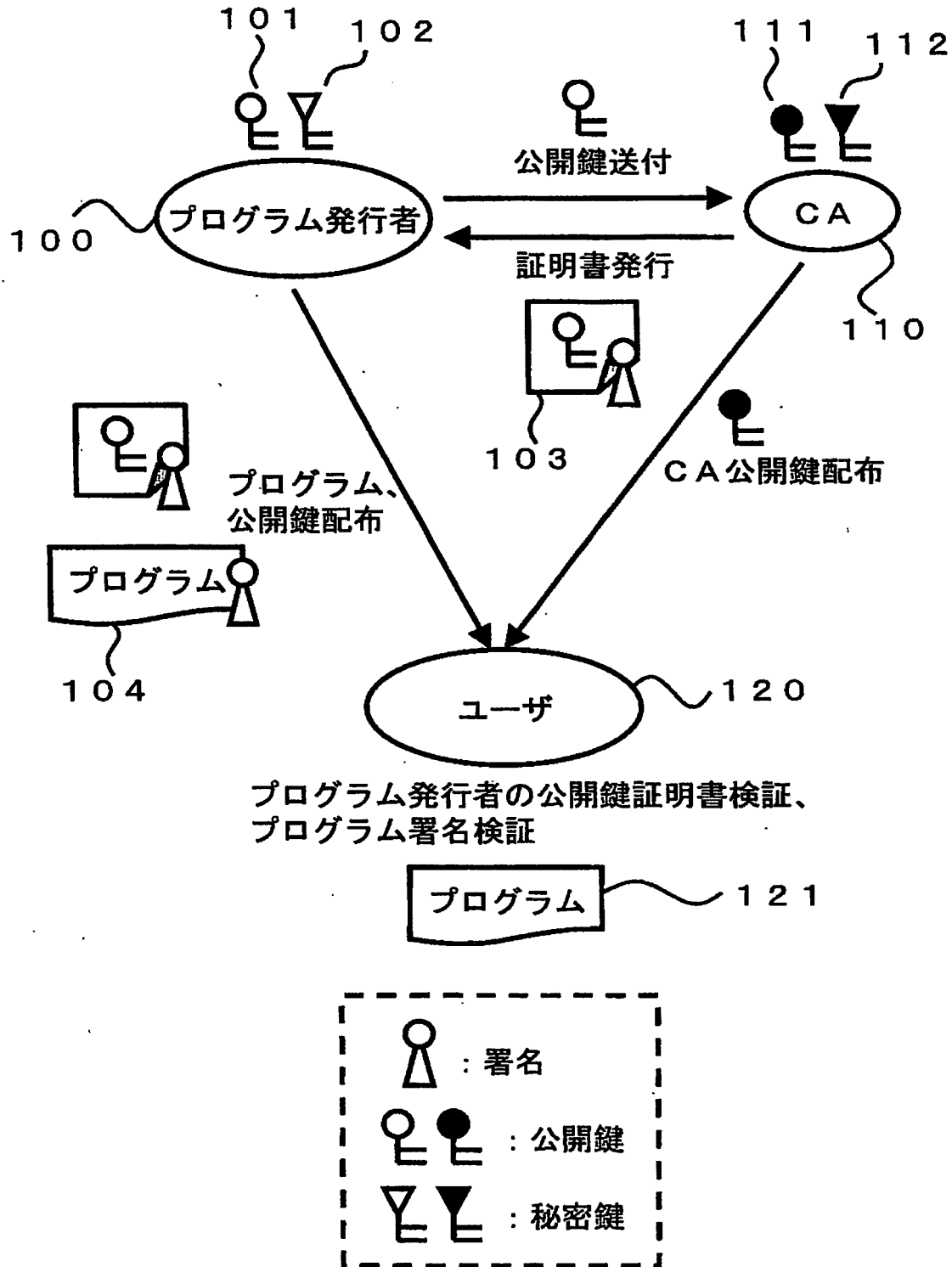
報ID

403, 703 固有情報数
404, 704 全体サイズ
405, 706 固有情報サブヘッダ
411, 711 プログラム固有情報サブID
412, 712 サイズ
705 プログラム固有情報ハッシュ値
840, 900, 1140, 1200 固有情報配布履歴
903, 1204 最終配布日付
1150, 1210, 1750, 1810 プログラム／固有情報対応表
1213, 1813 配布開始ID
1440, 1500, 1740, 1800 配布回数情報
1502, 1803 回数カウンタ

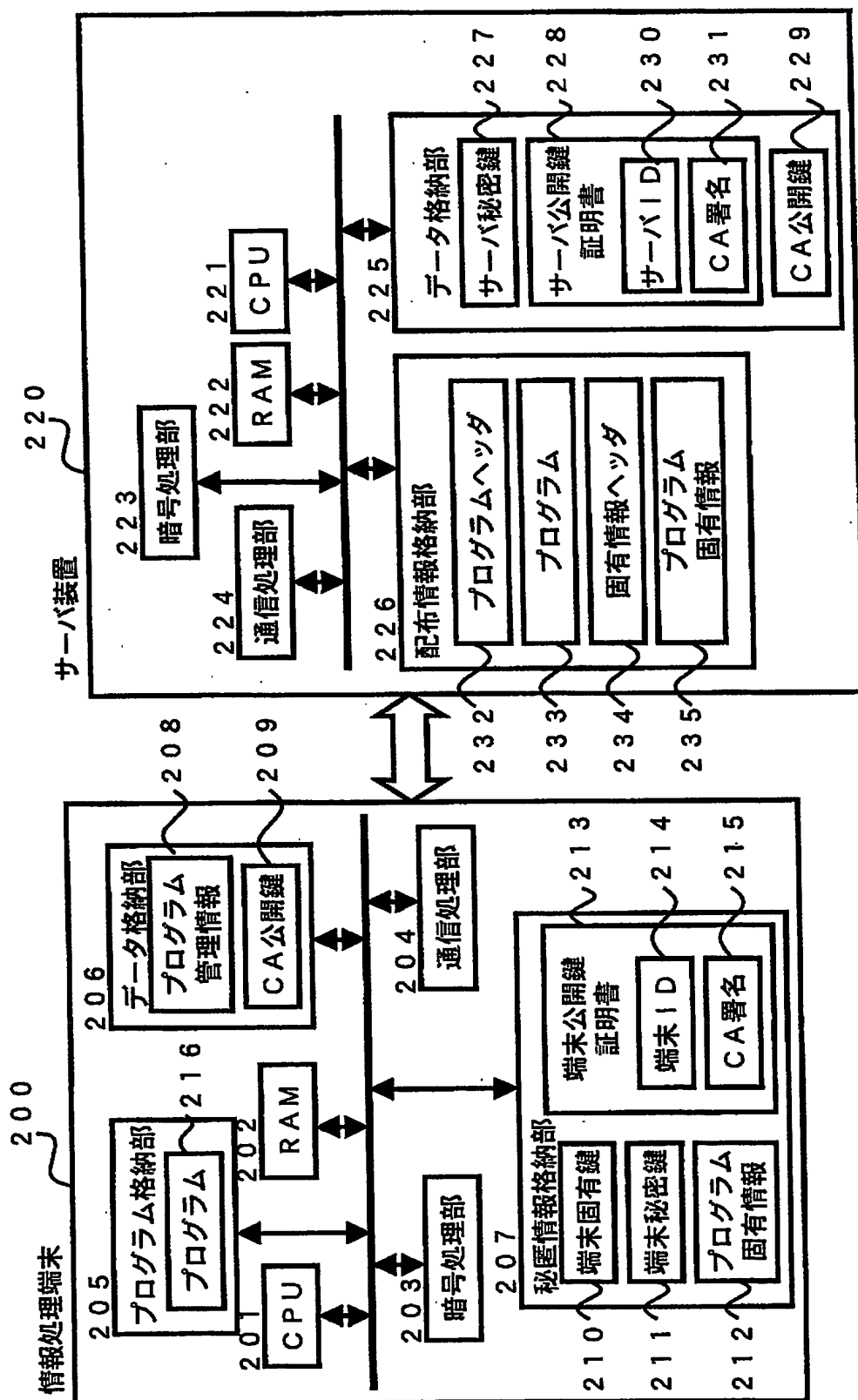
【書類名】

図面

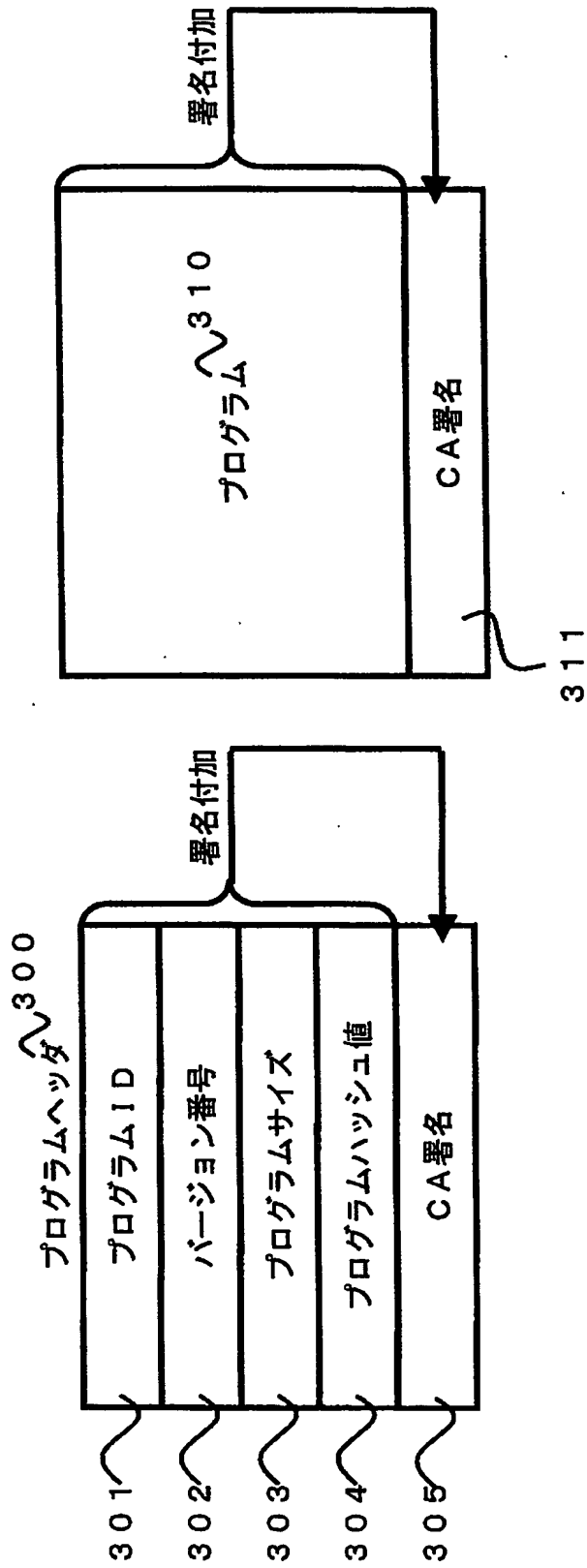
【図1】



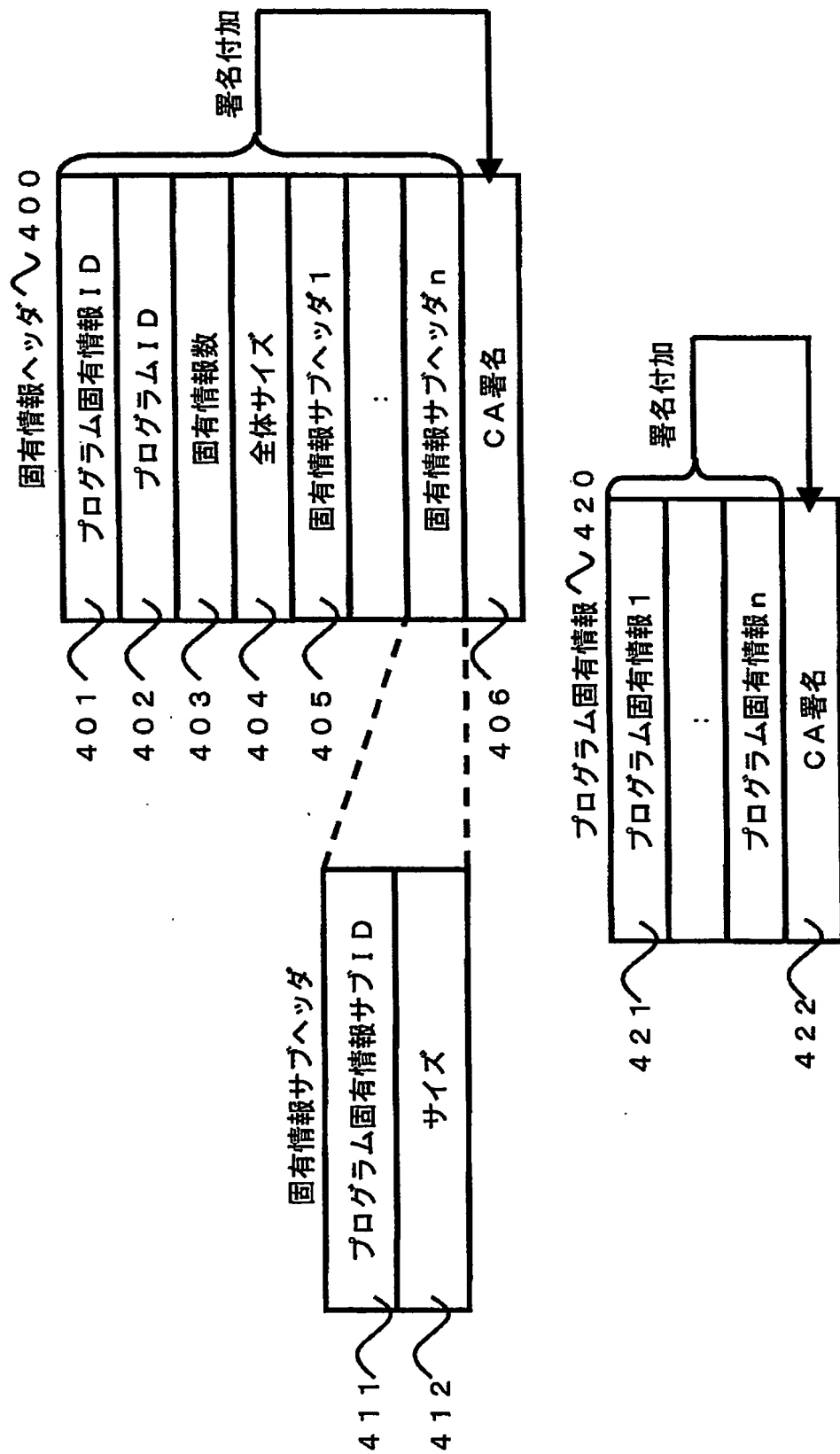
【図 2】



【図 3】



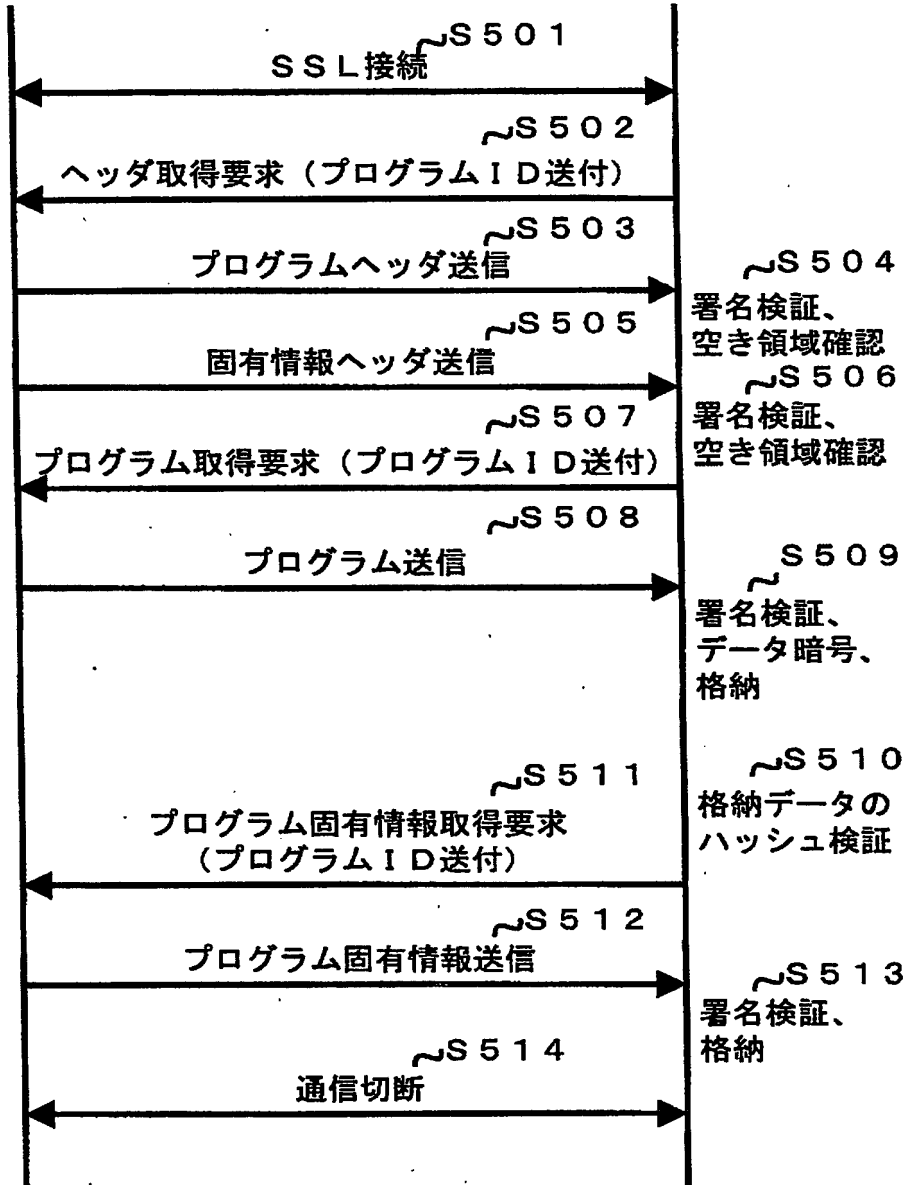
【図 4】



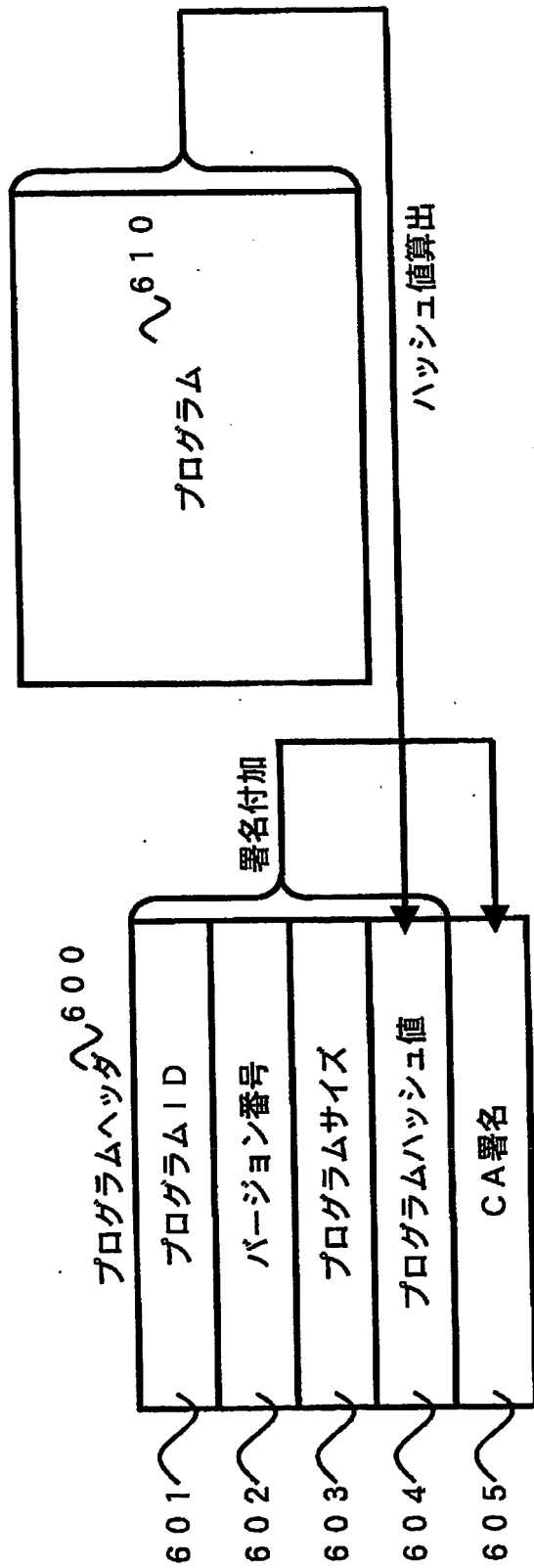
【図5】

サーバ装置

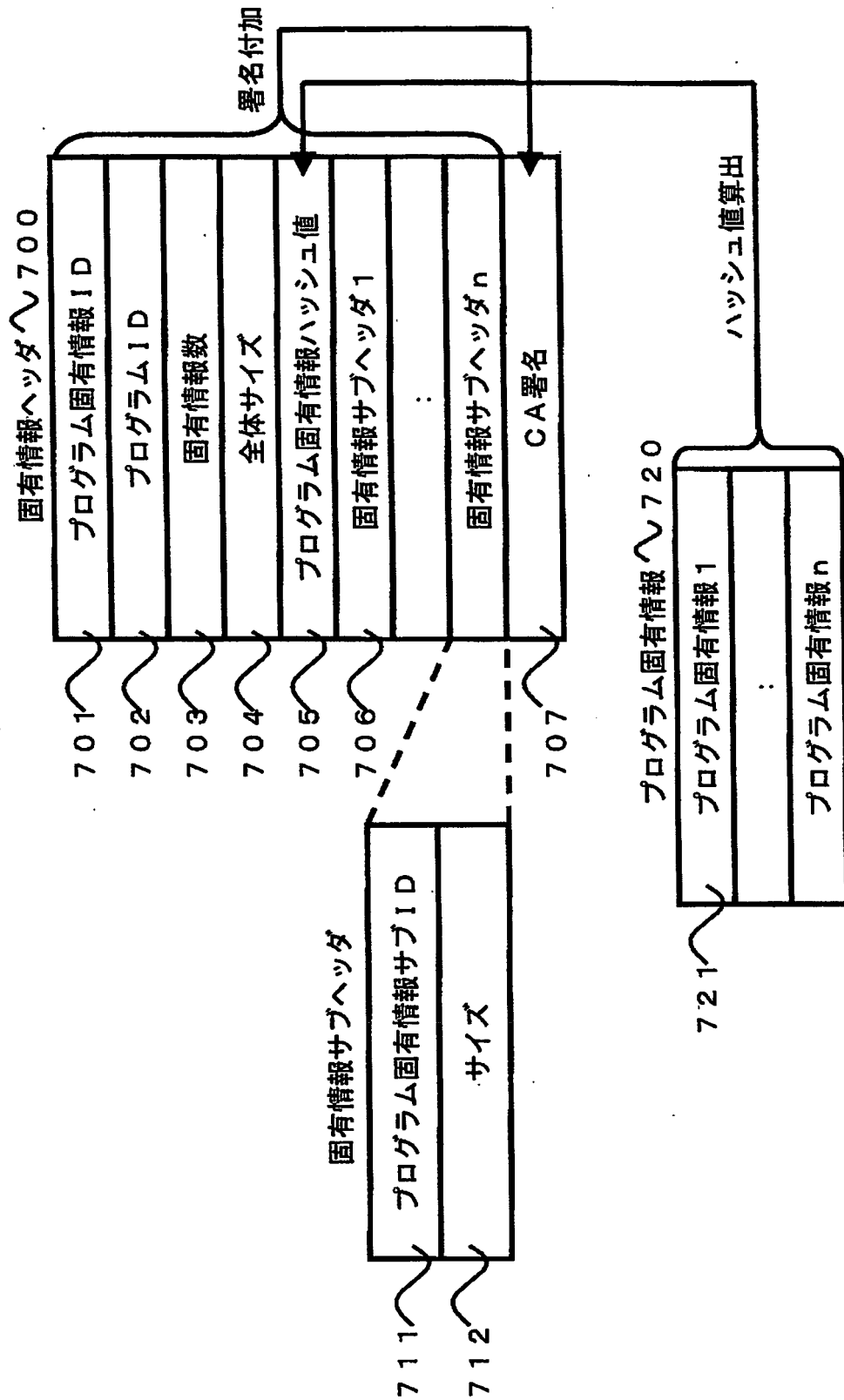
情報処理端末



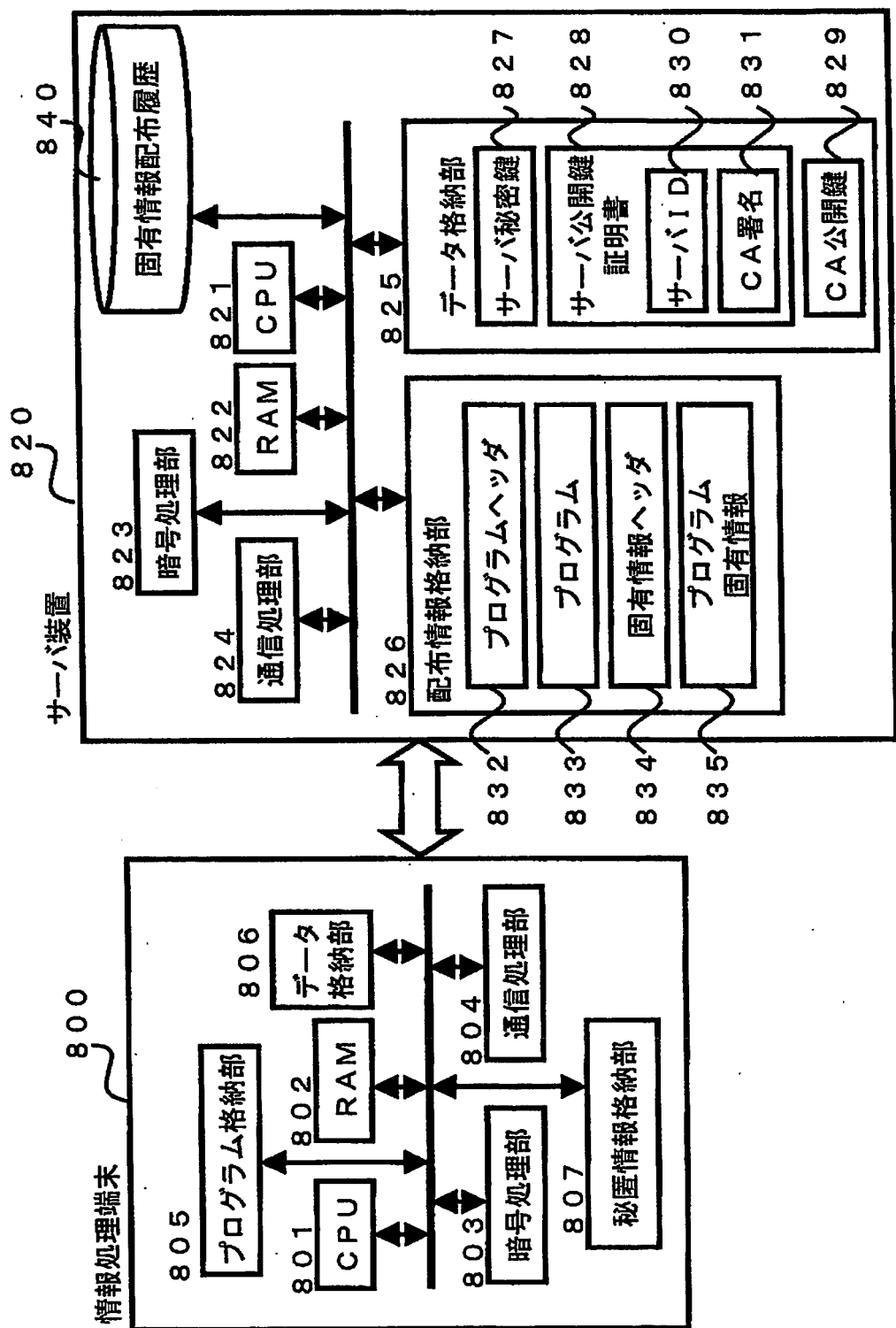
【図6】



【図 7】



【図 8】

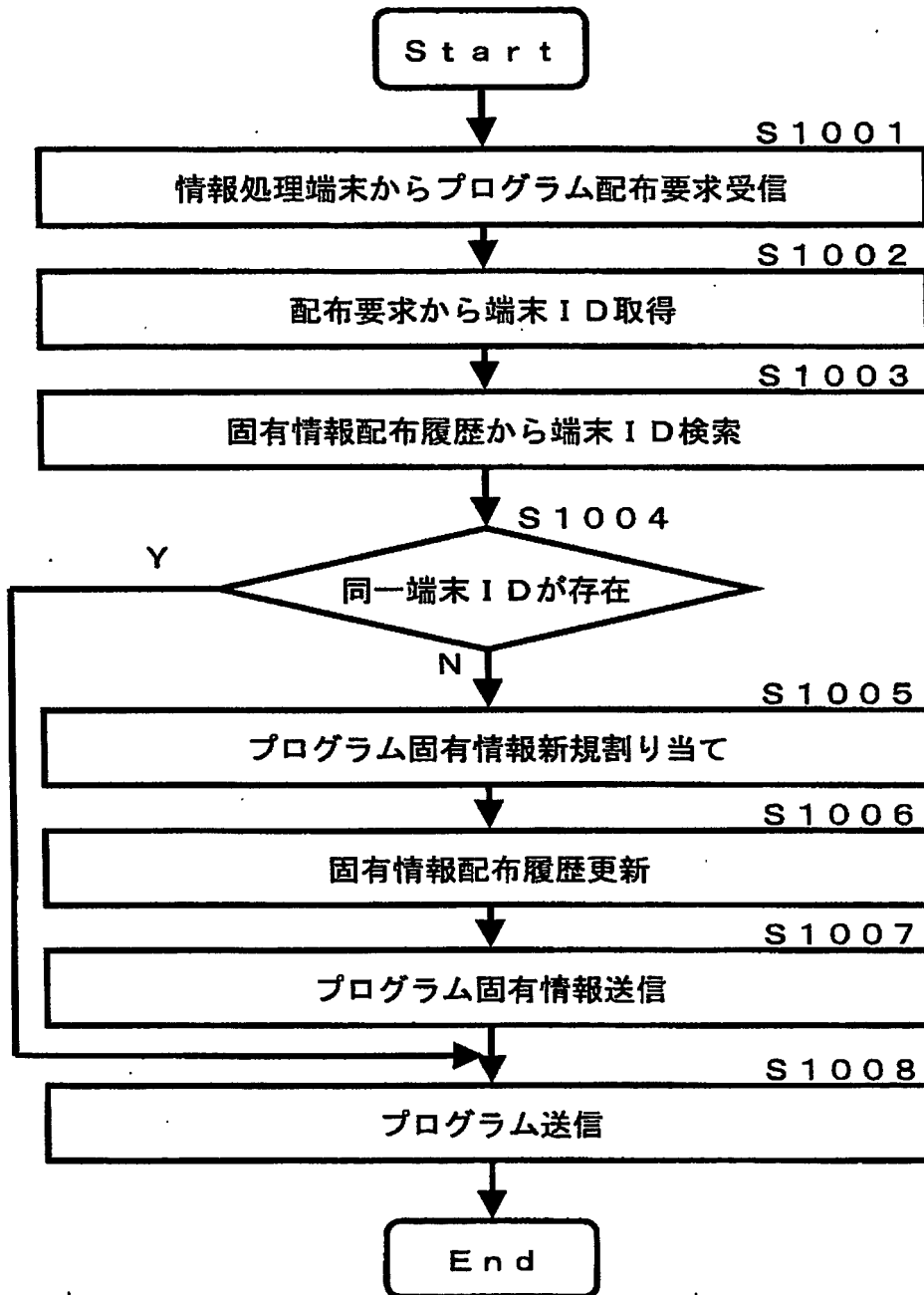


【図9】

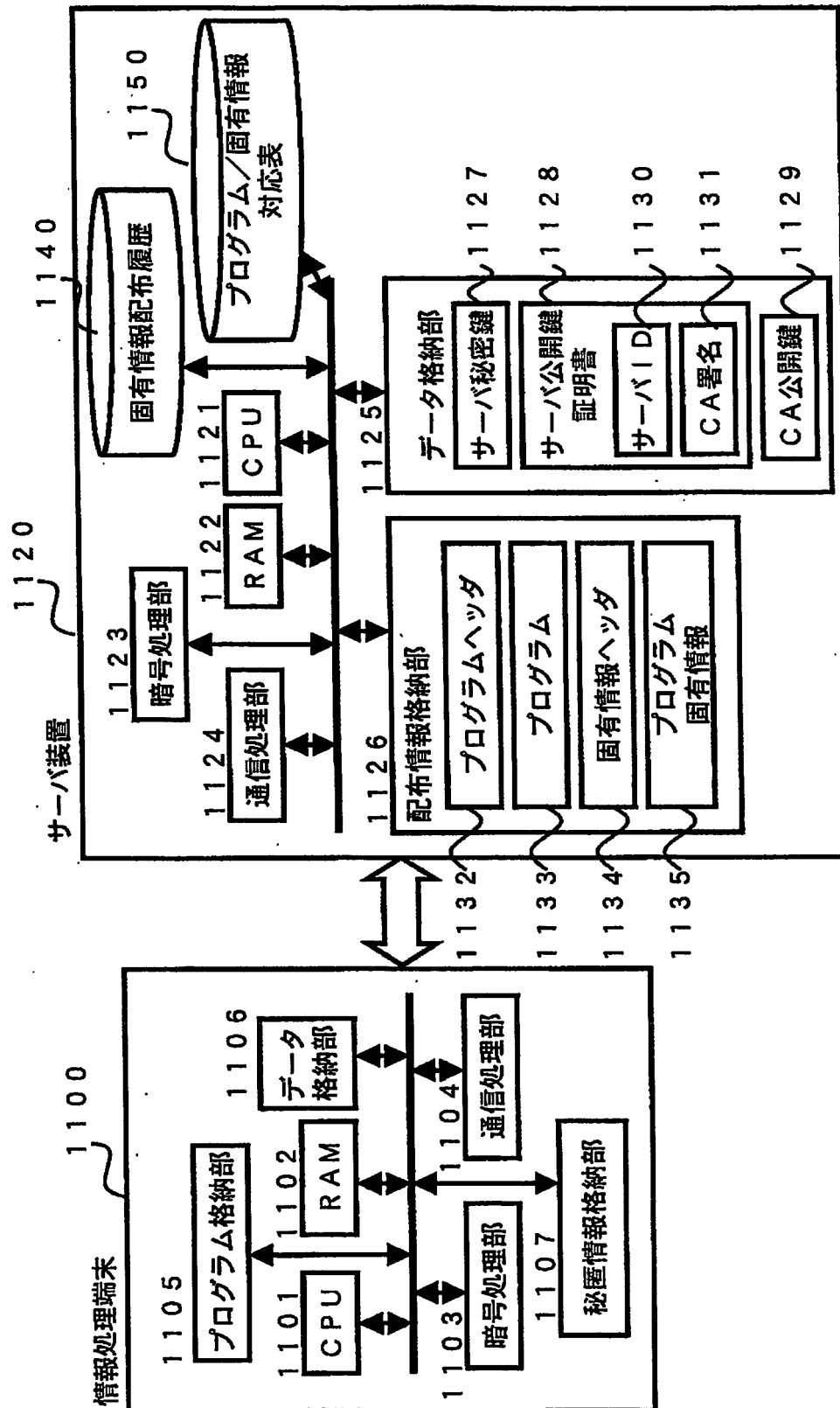
固有情報配布履歴 900

901 端末ID	902 プログラム 固有情報ID	903 最終配布日付
0001	0001	2002. 3. 12
0002	0002	2002. 3. 12
0010	0003	2002. 3. 13
0015	0004	2002. 3. 14
0020	0005	2002. 3. 14

【図10】



【図 11】



【図 12】

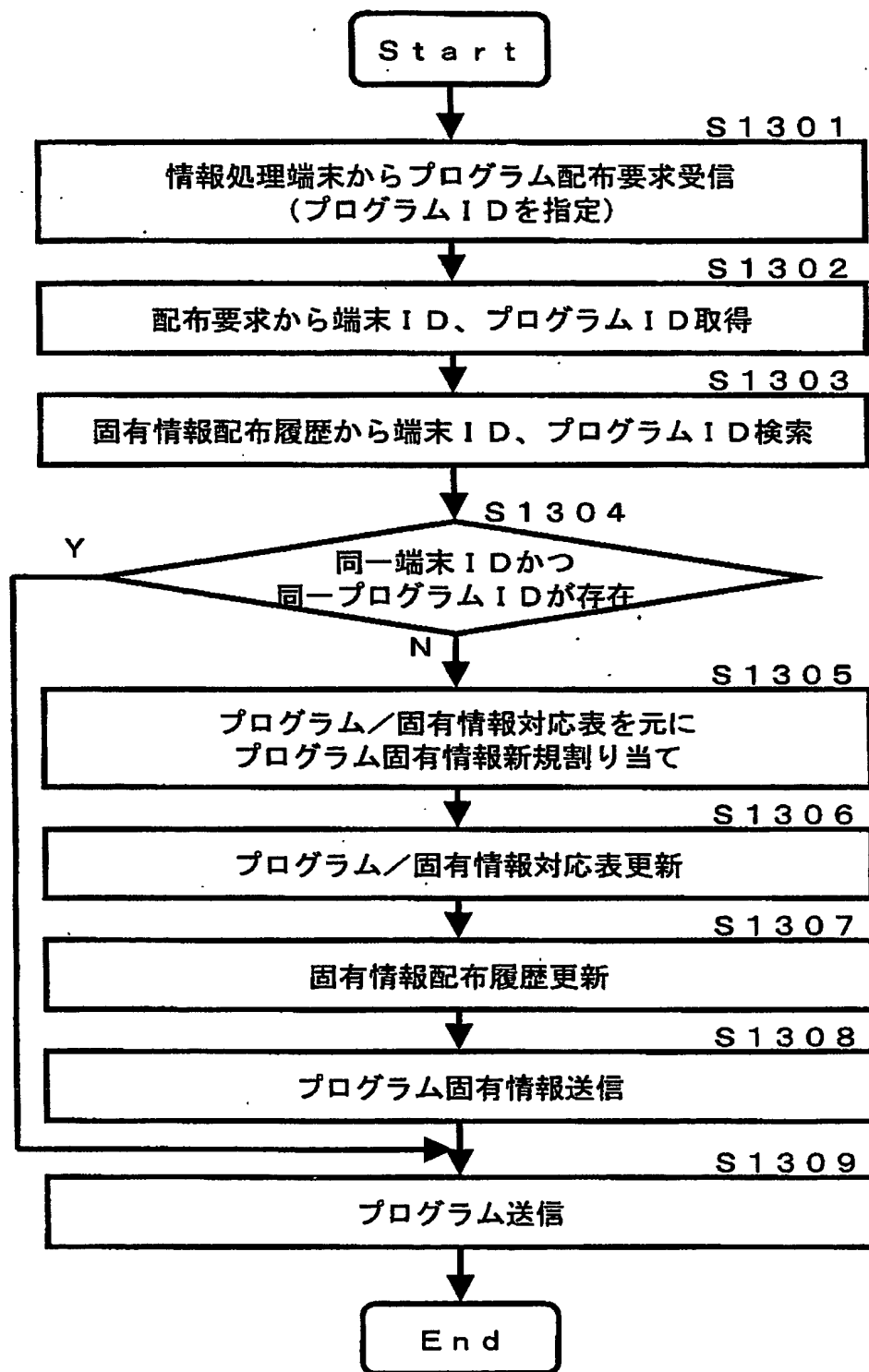
固有情報配布履歴 1200

1201 端末ID	1202 プログラムID	1203 プログラム固有情報ID	1204 最終配布日付
0001	0001	0001	2002. 3. 12
0002	0001	0002	2002. 3. 12
0010	0001	0003	2002. 3. 13
0015	0001	0004	2002. 3. 14
0020	0002	1001	2002. 3. 14

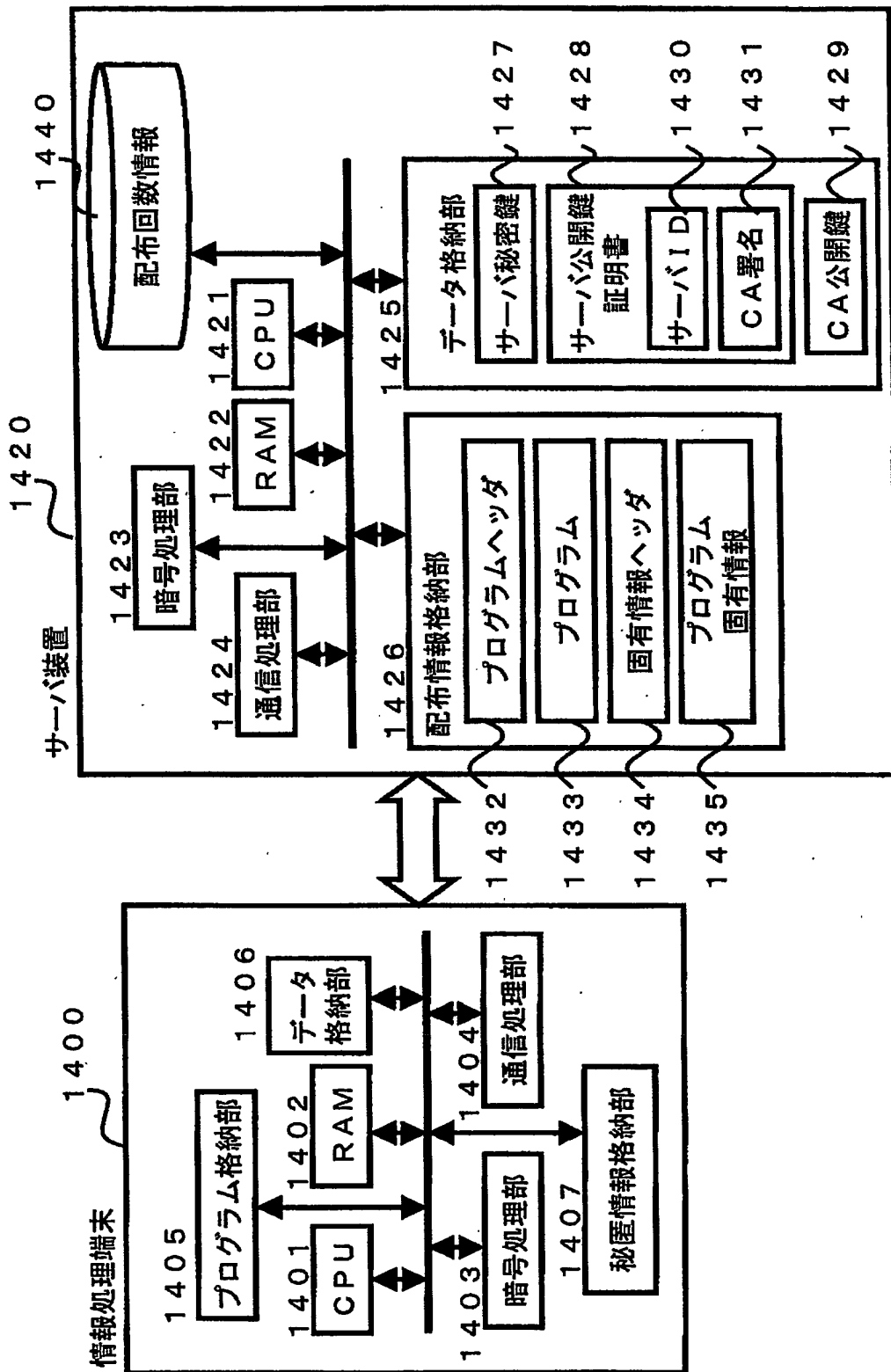
プログラム／固有情報対応表 1210

1211 プログラムID	1212 プログラム固有情報ID	1213 配布開始ID
0001	0001～1000	0123
0002	1001～2000	1423
:		

【図 13】



【図14】



【図 15】

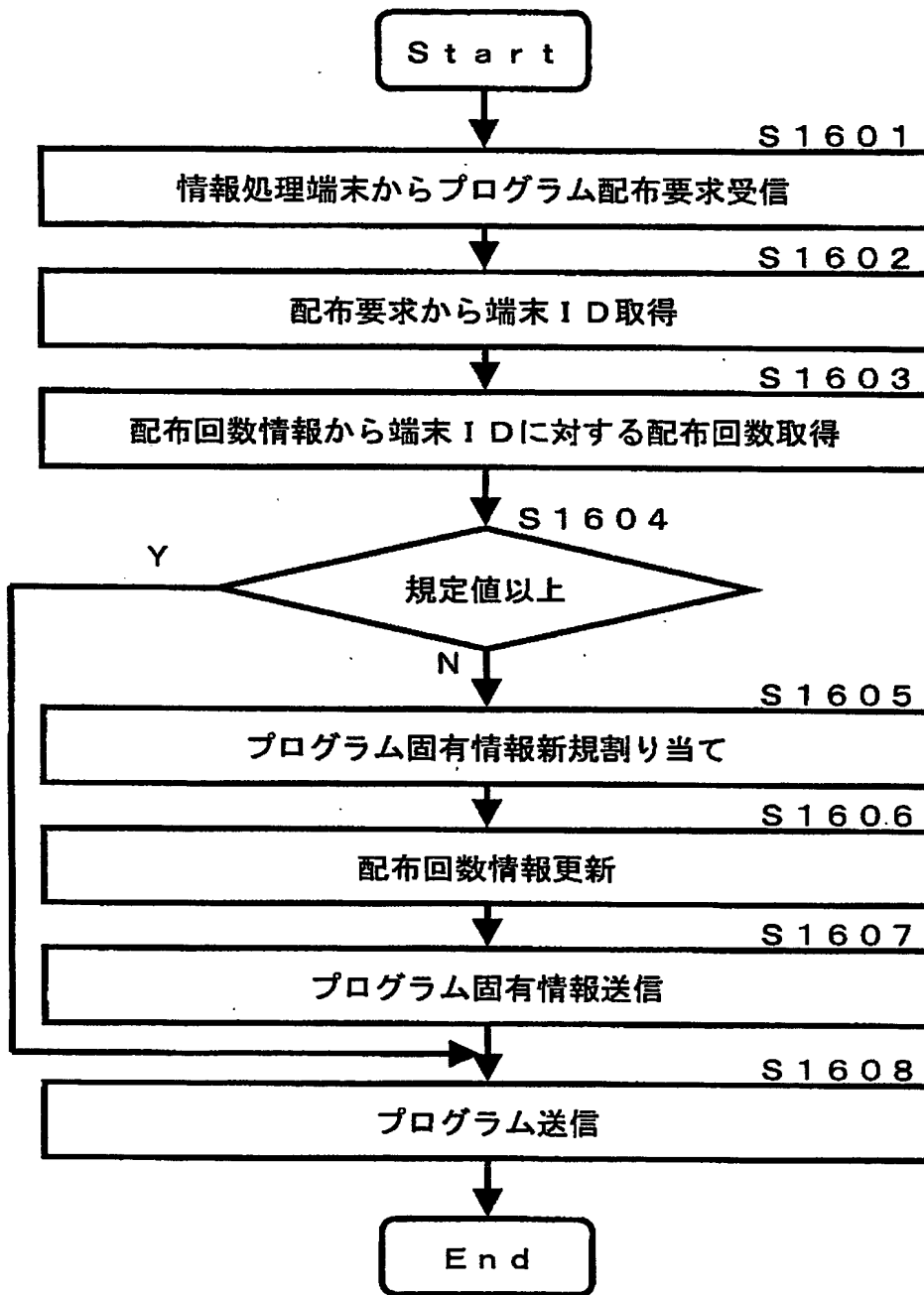
配布回数情報

1500

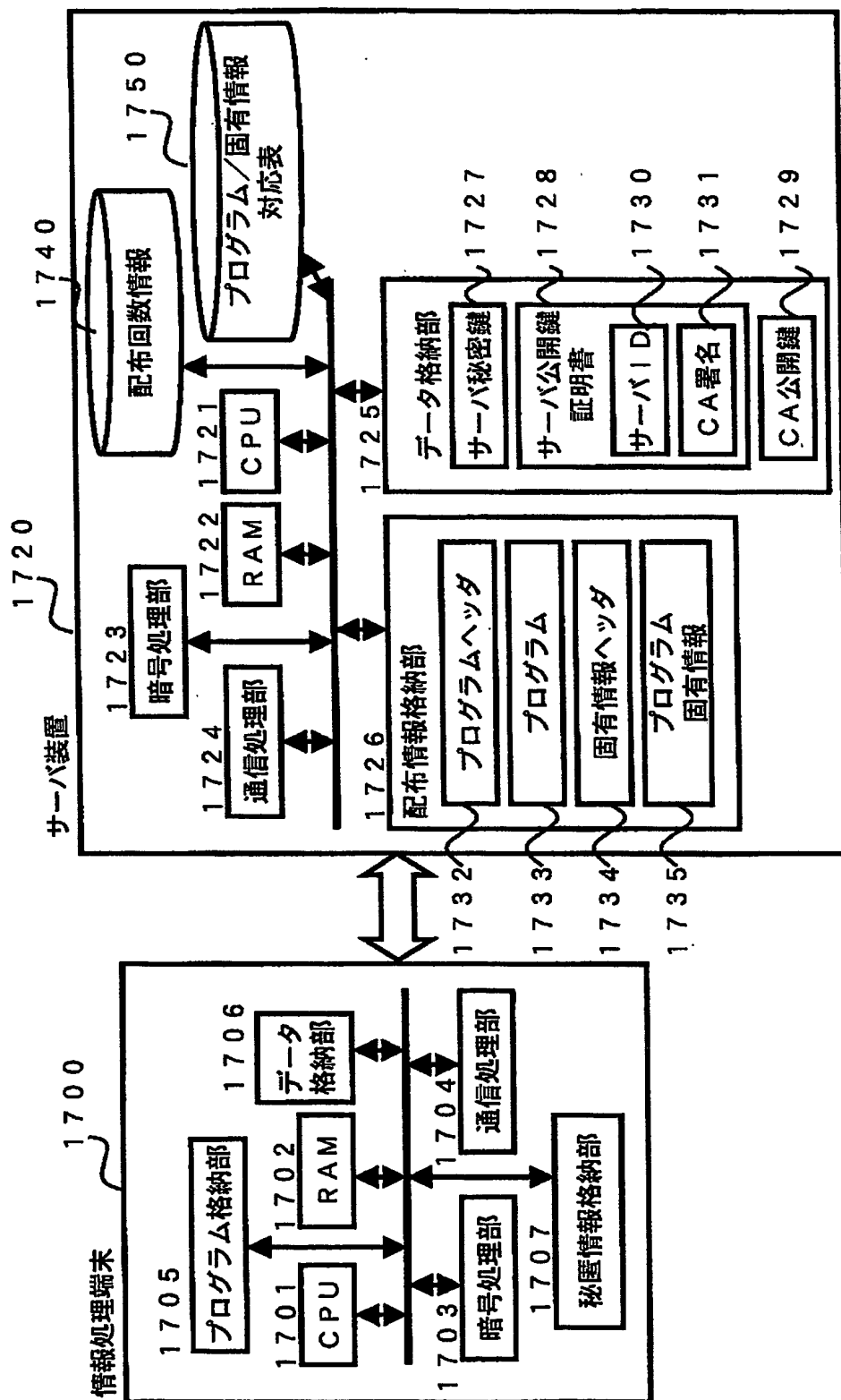
1501 1502

端末ID	回数カウンタ
0001	1
0002	1
0003	0
:	

【図 16】



【図 17】



【図18】

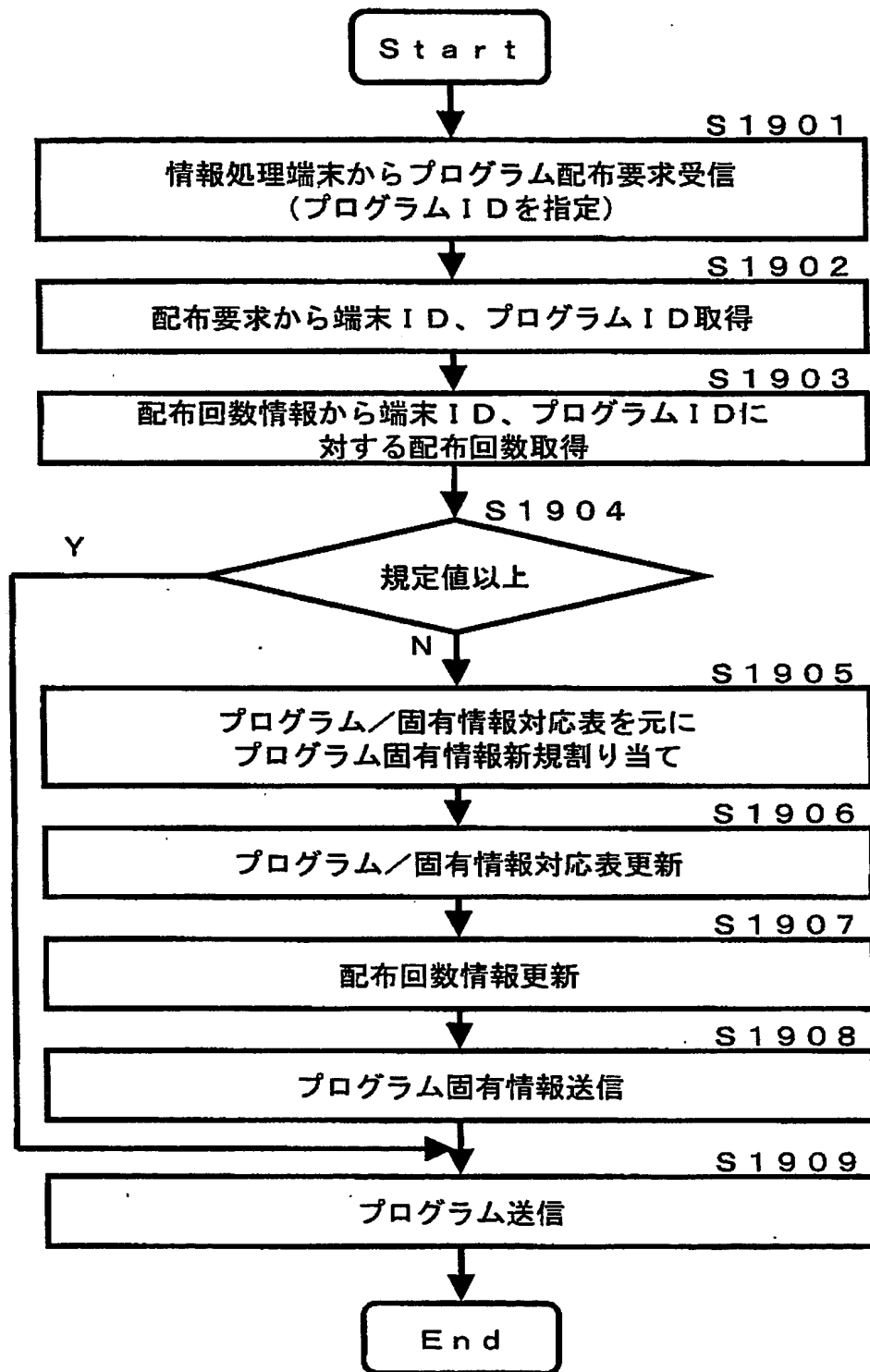
配布回数情報 1800

1801 プログラムID	1802 端末ID	1803 回数カウンタ
0001	0001	1
0001	0002	1
0001	0003	0
0002	0001	1
0002	0002	0
0002	0003	0
:		

プログラム/固有情報対応表 1810

1811 プログラムID	1812 プログラム固有情報ID	1813 配布開始ID
0001	0001~1000	0123
0002	1001~2000	1423
:		

【図 19】



【書類名】 要約書

【要約】

【課題】 プログラムをサーバ装置から配布する場合に、サーバ装置の負担を軽減し、プログラムの不正コピーや不正改ざんを防ぐと共に、不正行為を防止することが可能なプログラム更新及び管理方法を提供する。

【解決手段】 サーバ装置から配布されたプログラムを情報処理端末において、端末毎に異なる固有鍵で暗号化して格納する。このとき、平文プログラムのハッシュ値を用いて固有鍵への暗号化が正常に行えたことを確認する。また、固有情報配布履歴をサーバ装置が保持することにより、複数のプログラム固有情報を1台の情報処理端末に配布することを防ぎ、不正行為を防止することが可能となる。

【選択図】 図 1 1

出 願 人 履 歴 情 報

識別番号

[000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社